Unmanned Aerial Vehicles:

Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace

by

Evan Baldwin Carr

evancarr@dronejustice.com

Table of Contents

List of Abbreviations

ACLU – American Civil Liberties Union

ARC – Aircraft Rulemaking Committee

ATC – Air Traffic Control

CBP – Customs and Border Protection

CDL – Common Data Link

COA – Certificate of Authorization

DARPA – Defense Advanced Research Projects Agency

DOT – Department of Transportation

FMV – Full Motion Video

FBI – Federal Bureau of Investigation

FLIR – Forward Looking Infrared Imaging

ICAO – International Civil Aviation Organization

MPS – Minimum Performance Standard

NAS – National Airspace

NOAA – National Oceanic and Atmospheric Administration

RVT - Remote Viewing Terminal

SLAR – Side Looking Aerial Radar

sUAS – Small Unmanned Aerial System

TCAS – Traffic Collision Avoidance System

USCG – U.S. Coast Guard

UAS – Unmanned Aerial System (includes the UAV, pilot, ground control station etc...)

UAV – Unmanned Aerial Vehicle

USSOUTHCOM – U.S. Southern Command

VDL – Video Data Link

VFR – Visual Flight Rules

Introduction

The notion of unmanned aerial flight has existed far longer than most Americans realize. Having received considerable news coverage over the last decade since the start of the War on Terror, drone use has become a common sight on the battlefield. The expanding purview of unmanned aerial systems (UASs) raises valid regulatory concerns that have proven difficult to address. UASs, which include the unmanned aerial vehicle (UAV), the additional technical support structure and the pilot, will continue to be converted from military to civilian applications necessitating action by the regulatory agency vested with oversight to support the burgeoning unmanned aviation industry. Congress has granted this authority to the Federal Aviation Administration (FAA), mandating a timetable for UAS integration into the national airspace. Ensuring this is done safely to protect innocent Americans from preventable aeronautical accidents and infringements upon their civil rights is of the highest priority. As a global industry leader, it is important that the United States establish respected and effective standard operating procedures that will be a model for the many countries around the world adopting drones for similar non-military uses.

This paper will review the history of UAS development, consider the uses for UAS technology, examine the safety, insurance, security, privacy and regulatory issues associated with integration into the national airspace (NAS), and conclude with some recommendations.

Early UAS Development: 1900 – 1960

The early history of UAS development was sporadic, often taking place when armed conflict required that the military look for new technologies, only to have enthusiasm wane when the armed conflict ceased. The concept of remote pilotless vehicles was born during the early

days of electricity through a partnership between George Westinghouse and Nikola Tesla, the brilliant electrical engineer. He pioneered the remote control concept during the Spanish-American War, inventing a simple remote boat called the "Teleautomaton," which he implied could be used as a torpedo. As was frequent until the modern era of UAVs, military commanders failed to recognize the potential of unmanned craft (Newcome 2004, 11-14).

During the period from 1909 – 1920, scientific advancement of the aeronautical gyroscope by Elmer Sperry and airframe construction by Glenn Curtiss allowed these early pioneers to begin testing aerial torpedoes. These unmanned craft were not designed to return merely to fly to a target remotely and through various mechanisms, terminate forward velocity, dropping themselves, and presumably bomb payloads, on the targets. At this point, unmanned vehicles were not remotely controlled but controlled through a series of on-board devices with pre-set operations. In response to World War I, the aerial torpedo concept underwent rigorous testing and a brief production run was overseen by Charles Franklin Kettering. The Kettering Bug's purpose was to fly 50 miles and deliver a 200-lb payload on a target. While the Bug fell far short of this mark and was discontinued as the war came to a close, it was nevertheless the first instance of an unmanned aircraft performing a pre-designated flight pattern successfully (Newcome 2004, 15-29).

As aircraft became consistent in taking off and remaining airborne after World War I**,** attention then turned to adding remote control ability. Radio engineers worked with Sperry to create the Messenger, the world's first truly remote controlled aircraft. Successfully achieving two-hour flights and 90-mile accuracy, the Messenger was built as a relay vehicle and in an aerial torpedo configuration for the Army. The Navy was working on a similar project but by 1926 interest and funding disappeared as privatization of air freight transportation required

piloted flights (Newcome 2004, 31 – 39).

Across the pond the United Kingdom had been pursuing an unmanned aerial flight program throughout this early period. Development during the teens and twenties culminated with the DeHavilland Queen Bee, a target drone produced between 1934 and 1943, hence the apiarian UAS nickname "drone," which has stuck ever since**.** The Queen Bee inspired Hollywood actor and model airplane enthusiast Reginald Denny to invent the Radioplane-1 (RP-1) for gunnery practice and anti-aircraft military defense. At a cost of $600, more than 15,000 Denny Drones were used for training during World War II. The breakthrough UAV of World War II belonged to the Germans, who produced the V-1 cruise missile. Designed in 1940 and developed for a low cost, in the last 10 months of combat this jet engine airplane hit almost 25% of its targets, causing the Allies to lose 2,900 aircrew; a fact that led Allied forces to conclude that the V-1 offered a 4:1 return on investment (Newcombe 2004, 41 – 61).

At the same time target drones like the Queen Bee and the RP-1 were being developed, additional research during the late 1930s aimed at producing an aircraft that would not fly to a target and self-terminate but deliver its payload and return to base for future deployment. These more sustainable, higher longevity and higher altitude craft were quickly applied to the needs of the Cold War and a new mission was born: reconnaissance. Bearing familiar resemblance to modern UAVs, surveillance drones of the late 1950s and early sixties were being testing with "a 125-mm or a 70-mm film camera, flares for use with nighttime photography, an IR sensor," plumbing for dispensing chemical or biological agents from underwing tanks and a side-looking airborne radar (SLAR) that was capable of transmitting imagery back in real time via a ground sensor (Newcome 74). During this decade, the kinks in autonomous navigation were being worked out allowing an unmanned craft to auto correct its course and thereby ensuring accurate

navigation. Various schemes were tested, all ahead of their time, most prominently the perfection of the Inertial Navigation Systems of the ‘40s, the Star Tracker of the ‘50s and the Transit system of the ‘60’s, which was the first system to use satellite radio signals and which preceded GPS (Newcome 2004, 63 – 81).

Modern UAS Development: 1960 – Present

The Vietnam War marked a turning point for UAS development to support a variety of operations during the war. “1,016 AQM-34 Lightning Bugs and Firebees flew 3,435 sorties during which 544 were lost … for an overall mission success rate of over 84 percent” (Newcome 2004, 86). The ubiquity of the drones throughout the war and their various missions, from air defense and communication intelligence to leaflet dropping, solidified the functions of UASs in a modern military arsenal. High altitude and vertical lift-off drones were also developed during Vietnam but, typically, interest waned after the war and foreign UAV programs soon became global leaders. No country developed and employed UAV technology more prolifically than Israel which began research in 1970 and continued at a fervid pace (Newcome 2004, 83 – 91).

Based initially on a Firebee, the rapidly expanding Israeli aviation industry developed a number of decoys and observational drones that operated heavily in a region mired in political turmoil and war. During Operation Peace in 1982, aircraft over the Syrian-occupied area of Lebanon destroyed surface-to-air missile batteries by deploying unmanned decoys that the Syrians attacked, wasting resources and divulging the locations of the batteries for targeting by Israeli fighters (Sanders 2003). In the late ‘80’s and early ‘90’s, the United States renewed its interest in unmanned aerial systems after observing that “in both Lebanon and Syria, Israel was among the first nations to employ such vehicles regularly for reconnaissance in combat, demonstrating that when used effectively they can help achieve combat objectives” (Sanders

2003). As a close ally, the U.S. and Israel embarked on a program of joint development that ushered in the new age of unmanned aviation.

Working hand in hand, these two nations developed the Hunter and Pioneer UASs. The Pioneer was originally adopted by the Navy and was used effectively in the Gulf War to spot enemy fire for the delivery of munitions. It also operated in a surveillance function for the Marines during the 1994 Balkan conflict and in Kosovo in 1999 (Newcome 2004, 97). These battlefield successes heralded the drone as an effective combat tool, and it was during the 1990s that unmanned aircraft received significant media attention (Sanders 2003). Success on the battlefield and newly found public attention led a variety of interested parties to explore using UASs outside of their traditional military applications.

New scientific endeavors marked the transition of unmanned technology to the scientific sector, a development that led to great advances in military capabilities as well. Research in the 1990's focused on enabling the unmanned vehicles to stay airborne for periods over 24 hours and above 50,000 feet, on using new materials in the construction of the craft to make them lighter and stronger, and on harnessing solar power to propel the aircraft for indefinite periods of time (Newcome 2004, 118). NASA and the AeroVironment Corporation developed the solar-powered Pathfinder and Helios aircraft in the late 1990's. These UASs exemplified the technological advances being made at the time but were hindered by inefficient photovoltaic cells (DeGarmo 2004). Fully autonomous flights that included take-off and landing were pioneered, and for the first time the new Predator drone was outfitted with a laser-guided antitank missile, making it capable of patrolling, spotting, targeting and attacking at once (Newcome 2004, 110). With the advent of such technologies, it became clear that UASs in combat could lessen the need for manpower and put fewer soldiers in the line of fire. As the functionality and reliability of UASs

grew, the potential for their use in civilian and non-military government sectors became obvious.

Modern unmanned aerial systems would soon receive new widespread attention when the terrorist attacks of September 11, 2001 (9/11) changed the nature of war and their role in the ensuing conflicts grew. In this new age, the war waged was one against terror, illusive and cunning, difficult to track and impossible to eradicate. Al-Qaeda and their Taliban supporters soon met the force of the United States military response to the provocation of 9/11. Among the arsenal were newly retrofitted Predator drones equipped with Hellfire missiles**.** The first notable event in the new era of drone warfare occurred when a remotely controlled Predator drone located, tracked and fired a hellfire missile on a car, killing Abu Ali al-Hirithi, al-Qaeda's top operative in Yemen and one of the planners of the 2000 *USS Cole* bombing (Yoo 2011, 58). This notable strike was but the first of many UAS strikes that characterized military operations in Afghanistan and Iraq. In 2002, the CIA conducted a strike against Afghani warlord Gulbiddin Hekmatyar, who shortly after joining forces with the Taliban was killed by a drone (Yoo 2011, 59). In 2004, a "mysterious explosion" below Pakistani airspace killed Pakistani Taliban commander Nek Muhammad shortly after a drone was reported in the sky (Williams 2010, 874). This success in South Waziristan led to a Predator drone strike against Haitham al Yemeni (May 2004), a high-ranking Al Qaeda weapons expert, another strike against Egyptian-born number three in Al Qaeda, Abu Hamza Rabia (Dec 2005) and a strike against al-Zawaheri, Al Qaeda's number two operative, which missed its target destroying three buildings, eighteen civilians, including five women and five children enraging the Pakistani population (William 2010, 875).

The UAS targeting of enemy leaders and opposition troops has become a common practice in the Afghanistan and Iraq theaters of war since 2001. The New America Foundation (2013) estimates that since 2004, 420 drone attacks have killed between 2,000 to 3,200 militants

including 275 to 360 civilians. Miniature versions of larger UASs now inundate the field so extensively that "(n)ow there are thousands of small, unarmed aerial surveillance drones being used by troops on the ground—so many, in fact, that it is difficult to obtain an accurate estimate of their number" (Sharkey 2011, 229). These small UAVs can be deployed by hand and operated with an Xbox controller through a visual headset that allows troops on the ground to gain actionable intelligence at their command. While always somewhat controversial, uproar over drone assassinations reached new heights in October of 2011 when a lethal strike in Yemen killed Anwar Awlaki, a U.S. citizen and Muslim cleric accused of conspiring to carry out terrorist attacks against America (Cloud, Flieshman and Bennett 2011). In the first known case of the U.S. government killing a U.S. citizen with a UAS, "the raid also killed a second American, Samir Khan, who had produced virulent, English-language online propaganda for Al Qaeda" (Cloud, Flieshman and Bennett 2011).

Following the designation of the FAA by Congress to draft rules for civilian UAS integration into the national airspace, the months previous to this paper have witnessed increased drone coverage in the media. In April 2012, in the first ever event of its kind, an American citizen was arrested with the assistance of a UAS. When six cows wandered onto Rodney Brossart's 3,000 acre North Dakota farm, Brossart and his family chased police off of his land with high power rifles, believing they were entitled to keep the cows (Koebler 2012a). The ensuing 16-hour standoff ended when the Grand Forks SWAT team used a Homeland Security UAV to locate Brossart on the large farm and assist in his capture. Arrested for theft, criminal mischief and other charges, Brossart, who was sure UAV assistance in his capture was illegal, recently learned in August of 2012 that the charges against him would not be dropped (Koebler 2012b). Since the SWAT team did have a search warrant and the drone was used only for

surveillance, "District Judge Joel Medd wrote that 'there was no improper use of an unmanned aerial vehicle' and that the drone 'appears to have had no bearing on these charges being contested here'" (Koebler 2012b). The case could be in litigation for a long time if appellate courts decide to hear the case. (The Fourth Amendment issues that could be considered in this case are examined later in this paper on pages 21 – 25.)

Civilian Equipment and Operational Capabilities

As drone strikes have become one of the preferred tactics in the War on Terror, the possibilities for use in civilian and government sectors have not gone unnoticed. Civilian, educational and research applications coupled with an expanding need to fight terrorism at home has created regulatory hurdles that must be dealt with quickly in order to establish an environment conducive to this nascent industry. The following outlines the various non-military advances already in development or operational:

- *Agriculture and Wildlife:* UAS technology is being developed and applied to monitor soil erosion and crop maturity, mitigate frost apply fertilizer(UAV Marketspace Consulting n.d.). The Japanese were the first to apply UAV technology to the agricultural sector in 1986 when the government sponsored a competition to find a solution for the dwindling population of rice farmers (Newcome 2004, 127). Robotic helicopters now cover more than 10% of Japan's rice acreage and have driven an expanding UAV industry in Japan. Fuji Heavy Industries has developed the RPH2 and Yamaha the RMAX, both fully autonomous chemical sprayers whose pilots numbered more than 8,000 in 2007 (Nonami 2007, 124**).** Like the Japanese, General Atomics, a U.S.-based defense consortium, has partnered with NASA and the U.S. Department of Agriculture Forest Service (USFS) and UAV Collaborative to develop a forest fire

unmanned aircraft to improve the effectiveness of tactical firefighting. Airborne platforms, thermal infrared imaging technology and data telemetry will combine to reduce access time to critical fire map data. The technology will assist the USFS in wildfire management and researchers Ishutkina, Chan and Feron (2004) have already developed algorithms that can successfully track tagged wild animals and monitor wildlife inventory (UAV Collaborative n.d.). Johnson et al. (2003) successfully gathered high resolution vineyard and coffee field images that indicated crop maturity while Jensen, Zeller and Apan (2011) have demonstrated that UAVs are capable of flying predetermined flight paths and taking accurate pictures of target fields. UASs like the AeroView are economical for farmers who pay 25-50% less for a UAV to detect differences in crop growth and blight than a manned aircraft (Caumont 2005). Invasive plant species may also be assessed (NASA 2004). Saving both money, time and potentially lives, unmanned applications in agriculture and wildlife conservation will put more UAS in the sky.

- *Earth Science* : NASA (2004) predicts that UASs will help scientists augment but not replace existing satellite functions, allowing for more accurate data sets. UAV capabilities might include measurement of geophysical processes associated with natural hazards like earthquakes and volcanoes; aerosols and gas levels in clouds; changes in the stratospheric ozone chemistry; tropospheric pollution and air quality; water vapor; changes in the composition, vegetation, coral reefs and nutrients of coastal zones; emissions from fires and volcanic plumes; oxygen and carbon dioxide levels in the air; vegetation structure, composition and canopy chemistry; glacier and ice sheet thickness and surface deformation; radiation levels; topographic mapping;

gravitational acceleration; magnetic fields; the Antarctic; cloud microphysics; river discharge; soil moisture and freeze/thaw states; extreme weather observation and forecasting; hurricane genesis; evolution and landfall and physical oceanography; meteorology and atmospheric chemistry (NASA 2004).

- *Homeland Security*: In the post-9/11 security environment, demand for domestic surveillance will drive a majority of UAV market (Frost and Sullivan 2003). Currently, many of the homeland defense UASs in regular operation are maintained by Customs and Border Protection (CBP) along the United States border with Mexico and Canada. Directed by Congress to acquire and operate a fleet of UASs, the CBP Predator Bs have been noteworthy in filling the gaps in border surveillance along difficult terrain, offering more sustained border coverage and reducing the risk to border agents (Haddal and Gertler 2010). Equipped with similar infrared and high resolution imaging, U.S. Southern Command (USSOUTHCOM) in co-operation with El Salvador has already demonstrated that unmanned craft can be effective in maritime surveillance (Padgett 2009). The Heron, developed by Israeli Air Industries and Raytheon, successfully monitored a drug smuggling ship off the Pacific coast of El Salvador, leading to the first apprehension of its nature. The Coast Guard, realizing the ability of UASs to monitor vast stretches of territory, has sought UAS technology since the initiation of its failed 2007 Eagle Eye program and is now working jointly with the U.S. Navy and CBP to develop its UAS program (USCG 2012). The Department of Defense has found it feasible for unmanned aerial systems to conduct surveillance of the open ocean, portable foreign WMD capabilities, mines, and subsurface, surface and air threats to our nation's ports (Healey et. al. 2007). In

addition to these homeland security applications, unmanned craft may also replace manned craft in evaluating pipeline threats (Gleason et al. 2011).

- *Civil Government*: Ordinary citizens will encounter UAS primarily through deployment by law enforcement agencies. Among the new technologies being equipped, the Army is heavily researching facial recognition software, forward looking infrared imaging (FLIR) and behavior analysis programs (Shactman 2011). Despite the privacy concerns and fears of an Orwellian police state that employs an army of drones to watch over every citizens' every action, drones are being vetted as the next logical technological innovation in law enforcement. Drones have been suggested to assist police personnel in locating and responding to emergencies, conducting surveillance, assisting search and rescue operations particularly during inclement weather or treacherous terrain, traffic monitoring and nuclear, biological and chemical sensing and tracking (DeGarmo 2004). Civil government drones could aid in mapping the extent of floods and flood damage, mapping land use, monitoring chemical and petroleum spills, relaying communications and monitoring sensitive sites.
- *Commercial*: Manned commercial airliner flights may never be fully automated given the number of lives aboard commercial jets but a host of other manned aircraft may be replaced by drones in the commercial sector. This includes filming for the motion picture industry, relaying communications, acting as surrogate satellites, inspecting utilities including power lines, dams and bridges, supporting the news and media industries, aerial advertising, spotting fish for commercial operations, carrying cargo and commercial security applications (DeGarmo 2004).

Market Forecast for UAVs

While it is impossible to note every potential civil application of UAV technology given the experimental nature and stage of development of the industry, the blossoming uses for UAS technology mentioned above cover most of the anticipated real-world applications. The wide variety of applications outside the military sphere forecasts growing civilian and government fleets that will create substantial regulatory, technical and privacy hurdles that must be overcome before UAVs can be successfully integrated within our current systems. UAV market projections vary slightly, but all projections are for a continuation of the current trend of a rapidly growing market. The Teal Group, an aerospace and defense market intelligence firm, estimates that annual global UAV spending will grow from $6.6 billion in 2012 to $11.4 billion in 2021, almost doubling and totaling just over $89 billion in the next decade (PR Newswire 2011). Lucintel, a global market research firm, has a lower estimate of the current market, placing it between $5 billion and $6 billion by 2016 (Lucintel 2011). They predict that the U.S. will drive a majority of the market, followed by France and Germany -- which have set the pace in Europe -- and Israel -- which presently leads the Mid-East. They note a high growth potential for the Asia-Pacific region.

Safety Issues

The National Airspace System facilitates air transportation and sets forth the rules by which aircraft operate. It “is the collection of procedures, regulations, infrastructure, aircraft, and personnel that compose the national air transportation system of the United Sates” (Wiebel and Hansman 2005). The introduction of UASs into a system that has traditionally been dominated by manned flights creates a number of safety issues, including potential air collisions, ground

collisions and system reliability.

UAS operation within the air traffic control system (ATC) differs from the established manned flight system in that unmanned vehicle control and traffic avoidance are functionally different. In traditional aircraft, ATC will issue a command for the pilot by radio and the pilot will adjust to avoid collision (Wiebel and Hansman 2005). In addition to ATC, pilots have two methods of spotting and avoiding aircraft: either by visually detecting a potential collision or the Traffic Collision and Avoidance System (TCAS), which compares local air traffic transponders to the unit's altitude and warns of potential collisions (Harlem 2012). In order to avoid collisions, UASs must have the same ability to detect-and-avoid as other aircraft while moving through the air. Different methods of vehicle control have all been tested, from completely autonomous flight to direct input by an operator, as well as a variety of traffic surveillance methods including ATC or plain eyesight. (Wiebel and Hansman 2005, 30). Billingsly (2006) has proven that TCAS significantly lowers the risk of mid-air collisions for the Global Hawk, a large UAS deployed primarily by the Air Force and Navy. Regardless of the avoidance system used, it is "likely to be required for all UAVs that operate within the boundaries of airways and on the same flight levels as current traffic at both high and low altitudes. This may either be provided by air traffic control or by a form of active collision avoidance by the UAV system" (Weibel and Hansman 2005, 77). The requirement dictating the see-and-avoid ability must be translated into a Minimum Performance Standard (MPS). "This MPS should be sensitive to and flexible enough to account for the range of UAV types, missions, and operating environments" (DeGarmo 2004). Since UAS flights will cross international borders, it is important that regulations be adopted by an international regulatory agency to ensure uniformity. The International Civil Aviation Organization (ICAO) would be the most likely body regulating unmanned civil drones and it has concluded that currently unmanned flight is permissible within the established "rules of the road" in international airspace (Marshall 2010).

Marshall (2010) comments that it will still be difficult for international UAS operations given the inconsistencies between states and governments over UAS operation. Ensuring that UAV operators around the globe operate by the same standards will mitigate any potential risks of mid-air collisions.

Potential impacts with the ground can be equally as dangerous as mid-air collisions. If a UAV system fails, impacts a populated area and the debris penetrates shelters, it is possible that the public on the ground could be fatally injured. All flights, manned or unmanned, are associated with some risk, but Wiebel and Hanson's ground impact model predicts a low risk of catastrophic accidents after accounting for population, debris size, vehicle reliability and the previous incidence of failure (Weibel and Hanson 2005, 68). As expected, they note a higher risk around more heavily populated cities like New York, Chicago and Los Angelos. They conclude that smaller UAVs could fly over 95% of the country with little risk while larger UAVs could fly over 20% of the country and meet the current established levels of risk if the vehicles could operate around 100,000 hours between accidents, the current standard for aviation safety. According to testimony from Nancy Kalinowski, FAA Vice President for System Operations Services, "the CBP accident rate is 52.7 accidents per 100,000 flight hours. This accident rate is more than seven times the general aviation accident rate (7.11 accidents/100,000 flight hours) and 353 times the commercial aviation accident rate (0.149 accidents/100,000 flight hours)" (Kalnowski 2010). While accidents do not necessarily predict collisions with the ground or other airborne objects, the high accident rate among CBP Predator Bs suggests the need for current safety levels to be increased before full integration into the national airspace.

In order to meet and exceed acceptable levels of risk, the reliability of UAVs must be increased**.** "Improving reliability is a recognized goal of the UAV community and is being actively pursued by aircraft manufacturers...there are essentially two ways to improve reliability: 1) improve the integrity of components and systems and/or 2) build in redundancy" (DeGarmo

2004).

Ensuring that UAVs fail less often and when they do, that backup systems are able to recover the craft and complete the mission is necessary if UAS technologies are to make the transition from the battlefield, where casualties are expected, to civil skies where a voting and wary public is not ready to accept such loses. As such, investments of more than $1 billion dollars have been made in the areas of data link and ground control stations in 2010, according to Frost and Sullivan, a respected business research & consulting firm (Keller 2011). As far back as 2002, Shane Dougherty, in a Defense Department funded study, indicated that latency (time delay) and frequency jamming have a direct impact on the accuracy of UAS operations. Despite the almost two decades of modern UAV development, research into the optimization of the link between the ground and the craft will continue until a fail-safe system, if possible, is perfected. In this case, technology is both the limiting factor and the solution to making UAVs safe to operate above the heads of innocent families.

Ultimately, safe UAV flights will be the most influential factor in introducing unmanned technology to civil airspace. Just as with the data link, the air traffic control system and mid-air collision avoidance will eventually become reliable within established levels of reliability and risk for manned aircraft. As air traffic control is upgraded to the next generation system, more advanced avionics and satellite-based systems will replace ground-based tracking and allow easier oversight of the NAS. While fatality risks can be mitigated by technological advances, errors in human judgment can be neither predicted nor utterly prevented. Given the wide variety of UASs, from micro-sized manual craft to medium- and high-altitude autonomous craft, variations in an operator's skills and situational awareness, potential air traffic controller errors and inclement weather, it is surprising "that the human influence in UAV accidents is

approximately 70 percent less on average than in manned aircraft (due to UAV automation capabilities) and therefore human/system interactions account for a proportionally higher degree of accidents" (DeGarmo 2004). One reason for this may be because "rather than receiving direct sensory input from the environment in which his/her vehicle is operating, a UAV operator receives only that sensory information provided by onboard sensors via datalink. Currently, this consists primarily of visual imagery covering a restricted field-of-view. Sensory cues that are lost therefore include ambient visual information, kinesthetic/vestibular input, and sound" (McCarley and Wickens 2004). While autonomous systems will generally require less hands-on interaction, the large difference in UAV size, type and mission means "there may not be a 'one size fits all' solution to the question of controller requirements. However, safety dictates two primary requirements for UAS pilots: they must be proficient in controlling the aircraft and interacting with other assets in the airspace" (Nas 2008, 17). This highlights the need for appropriate automation and ground training so pilots can safely avoid mid-air and ground impacts.

Insurance Issues

In order for UAVs to operate safely within the NAS, insurance must mitigate many of the civil liability concerns arising from flight. In the event ground damage occurs, Rapp (2010) believes that the flight operator will likely be responsible via strict liability, which considers aviation "'an ultra-hazardous activity' and actionable by way of strict liability, that is, without proof of a deviation from the standard of care...Injuries caused by UAVs crashing to the ground might also be pursued under products liability theories, including negligence, 'special' or strict liability, and various warranty claims." The identical principles, strict liability and negligence, would likely be applied to mid-air collisions and "many juries might be suspicious of UAV operations and unlikely to blame the pilots of other craft involved in midair collisions with

UAVs" (Rapp 2010, 635). Rapp (2010) concludes that the potential for communications interference could lead to common law nuisance claims and notes that the FCC has some regulatory hurdles of its own in sorting out which frequencies and bands UASs will use. Trespass and nuisance claims could potentially arise from low-flying UAVs, and environmental concerns open a host a lawsuits against potential operators (Rapp 2010, 645). For these reasons, "insurance costs were 85% of the cost per flight-hour, but only 24% of the total UAV flight service cost" according to a report prepared for NASA (Moire, 2004, 56). As reliability incrases with technological and safety innovations, costs will become more palatable for the future's potential drone operators.

Security Issues

In June 2011, a University of Texas at Austin research team hacked a Department of Homeland Security drone, bringing it under full control of the students and professor (NPR). Responding to a dare, Todd Humphreys and his team "spoofed" the UAV's GPS signal and took control of the craft in front of the operator's eyes. A wave of doubt arose within the industry and on Capitol Hill as it became evident drones were not fully secure. Even though the GPS was lightly encrypted, Humphrey's team hacked the GPS signal for less than $1,000. During testimony before Congress, Humphreys recommended that all UAVs over 18 lbs. be required to have anti-spoofing technology but rejected the idea that the military's existing anti-spoofing technology could be adopted given its exorbitant cost (Warwick 2012). Security of the ground control stations and data link infrastructure is a critical requirement for UAS integration. If UASs are easily manipulated by outsiders, the consequences could be grave. Terrorists could potentially use UAVs as flying missiles as in the September 11th attack, control them for surveillance use against us or any other imaginable use. With the expected number of civilian

and non-military governmental UAVs reaching 30,000 over the next five years, it is critical for the safety of our skies that these important security issues be addressed.

In order to make UAVs spoof-proof, new technologies would have to be included on-board that allow the UAS to detect modified GPS data. In testimony before Congress, Professor Humphreys offered a number of different solutions to work around the unsecured civilian GPS. His first suggestion is to include a Jamming-to-Noise sensor on board the craft which would detect a surplus in radio signals coming from the GPS spoofer and selectively ignore the additional false transmitted data (Humphrey 2012). Alternatively, he suggests encrypting the civilian Wide Area Augmentation System GPS signals which augment the traditional GPS system, adding multiple frequency receivers to the craft to receive multiple GPS bands, adding encrypted digital signatures into GPS navigation data or cross-referencing civil and military GPS signals (Humphrey 2012). The exploitable weaknesses of the current civilian GPS system present a clear danger for UAS operators and the public living beneath their wings. Additional precautionary measures must be taken before the scheduled full integration in 2015, preferably at minimal cost so as not to stunt the growth of the industry.

In addition to keeping the GPS signals free from interference, it is also necessary to completely secure the common data link (CDL) that connects the drone to the remote operating ground station and the pilot who controls it. Disrupted data links can occur maliciously and incidentally; both were common during the Afghanistan and Iraq actions.

> Remotely operated UASs require two separate radio communications links to operate: one communications link feeds (Full Motion Video) to a Remote Viewing Terminal (RVT) through a Video Data Link (VDL), the other communication link controls the UAS through a Common Data Link (CDL). The VDL uses an

> omnidirectional antenna to broadcast its communication feed in all directions, allowing any RVT tuned into the UASs VDL frequency to observe the UASs FMV. Video quality and consistency of reception relies upon the VDL signal strength. The CDL can use either an omnidirectional antenna or a directional antenna that broadcasts only in the direction of the Ground Control Station (GCS) (Yochim 2010).

Interference with either the VDL or CDL can occur naturally through the earth's or sun's electromagnetic emissions or through targeted jamming of the frequencies on which UASs operate (Yochim 2010). Yochim identifies three potential electronic warfare protections as spectrum management, electromagnetic (EM) hardening, and counter jammers, noting that while the vulnerabilities are easy to conceive, the solutions are more complicated, given the nature of aerospace engineering. By protecting the electromagnetic and frequency spectra, hardening the system through "filtering, attenuating, grounding, and bonding during the production process" or jamming the jamming frequencies, Yochim (2010) suggests that the CDL connections can be made secure and largely impenetrable, though it is worth noting that nothing is hacker-safe in relation to technology. The spillover rate of military technology to the civilian sector may dictate the speed with which civilian UASs are made safe. As with many technological innovations pioneered by the military, the civilian sector lags behind.

The speed with which non-military UAVs are made functionally secure may dictate their prevalence as governmental, scientific and commercial tools. Fixing the data-link and GPS issues are more important than making the craft fully operationally safe. A safe drone system will minimize the risks of fatal impacts and a properly trained operator will minimize the risk of human error but a drone susceptible to GPS manipulation and CDL interference could be more dangerous in destructive hands.

Privacy Issues

Completely safe and secure unmanned systems may be the inevitable result of technological advancements. Safety is less cause for alarm in the public eye than the potential privacy issues associated with drone operations. Successful drone missions operated by the CBP and U.S. Southern Command, a joint military command agency, have highlighted the applicability of UAVs in targeting drug smugglers and imply potential local law enforcement uses. In 2006, the Los Angelos police department tested a small UAS (sUAS), the SkySeer, for a variety of local functions, including hovering and watching a crime scene, tracking drug dealers, searching for lost children or Alzheimer's patients in difficult terrain, aiding police in pursuits and detecting speeders at a fraction of the cost of operating a helicopter (Bowes 2006). Since 2006, a handful of police departments all over the country have loaded up on a smorgasbord of different UASs while the drone industry is preparing to offer more than 18,000 police departments new UAS technologies (Bennet 2012). Many of the departments have not yet received a Certificate of Authorization (COA) and thus cannot operate their new machines. Following mass FAA authorization and before the swarm inhabits the skies, serious privacy concerns must be addressed to ensure that "Big Brother" does not become invasive and overbearing in violations of the Fourth Amendment.

The Fourth Amendment of the U.S. Constitution (Bill of Rights) guarantees that "(t)he right of the people to be secure in their persons, houses, papers, and effects of unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Some interpret this to say that people's privacy cannot be violated for any reason unless a warrant with probable cause is issued. Others believe that

privacy is not expressly protected by the Fourth Amendment. Fourth Amendment cases are common before the Supreme Court as innovations in technology and novel circumstances require deliberation by the ultimate judicial authority.

In examining case history relevant to drone surveillance and the Fourth Amendment, *Katz v. United States* (1967) established a standard that has withstood successive jurisprudence and been applied to emerging technologies. The *Katz* decision stated that a conversation inadvertently taped by law enforcement surveillance in a phone booth without a warrant that captured incriminating evidence was not admissible in court because "what a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protection. What he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (Katz v. U.S.1967). In what has become the standard Fourth Amendment litmus test, Justice Harlan "articulated a two prong test to determine when Fourth Amendment protection is appropriate: [1] a person must have exhibited an actual (subjective) expectation of privacy and … [2] the expectation must be one that society is prepared to recognize as 'reasonable'" (Troy 2009).

The first prong was subsequently struck down in *Smith v. Maryland*, an important implication for how future courts will decide UAV Fourth Amendment cases. In *Smith*, the Court upheld that a pen register that recorded the phone calls of a criminal did not qualify as a warrantless wiretap because he had no expectation of privacy since the calls could be accessed by the phone company (Smith v. Maryland). The case essentially struck down the subjective expectation of privacy and replaced it with an assumption that we are always being watched.

> Using the Smith logic, is a person's expectation to privacy in his or her personal back yard or curtilage illegitimate because, if a private third party

> could notoriously observe these areas, one must be "assuming" the risk of intrusive law enforcement observations? As aviation has advanced and has become more accessible to the public, the logical answer according to Smith is "yes." Also, could citizens lose their subjective expectation of privacy because the state gives them notice of no expectation of privacy in their backyard? Published post-Smith cases dealing with the collision between manned aviation, improved technology, and the Fourth Amendment unfortunately also answer "yes." (Troy 2009)

The cases following *Smith* included *Oliver v. United States,* when the Court upheld the open field doctrine, stating that which can be seen in plain sight is not protected by the Fourth Amendment and *United States. v. Dunn*, where the Court ruled that the Fourth Amendment applied to a person's curtilage based on "(1) the proximity of the area to the home; (2) whether the area is within an enclosure surrounding the home; (3) the nature and uses to which the area is put; and (4) the steps taken by the resident to protect the area from observation by passersby" (Oliver v. United States, United States v. Dunn). The progression of interpretation of the Fourth Amendment has already moved toward usurping an individual's rights over the burden of the state to provide evidence for searches in technologically enhanced situations.

Five important cases following *United States. v. Dunn* established additional precedents that will be important to the future discussion of an individual's right to privacy. *California v. Ciraolo* advanced the *Smith* logic and established that an individual's private property is not protected by the Fourth Amendment as long as the aircraft is in navigable airspace. The defendant in *Ciraolo* had built a privacy fence around his property but a pilot flew over his house and observed marijuana plants which led to a warrant and arrest. The Court ruled that even

though the plants were in his curtilage he had no expectation of privacy and that a “police officer does not have to shield his eyes when passing by and could traverse the airways like a typical aviator” (Troy 2009). The Court echoed this decision in *Florida v. Riley*, which concerned a helicopter instead of a fixed-wing aircraft, finding that curtilage was not protected from aerial view assuming that the aircraft was operating within established flight safety guidelines (Troy 2009). The third important case is *Dow Chemical Co. v. United States*, which challenged the legality of using aerial photography as incriminating evidence (Dow Chemical Co. v. United States). The Court found that use of photographic equipment was acceptable as long as the equipment was readily available to the public and that the enhanced photographic capabilities did not excessively intrude on privacy rights (Dow Chemical Co. v. United States). The fourth important case is *United States v. Torres*, which established that broad and indiscriminate video surveillance, like oral and wired communications, is a "hyper-intrusive search," and warrants greater scrutiny because: "[1] they are overbroad…; [2] they occur without notice; [3] they are ongoing; and [4] they pose an unusual threat to human dignity. Legislatures have taken notice, creating various statutes to control such searches” (Troy 2009). The fifth important case following *United States. v. Dunn* was *Kyllo v. United States*, in which the Court held that extra-sensory equipment like a thermal imaging device constituted an invasion of privacy but left open a loophole allowing equipment available to general public to be used without a warrant (Troy 2009, 15).Together, these Fourth Amendment cases give some indication of what will be constitutionally allowable in regard to where UAS surveillance ends and privacy intrusion begins.

A number of questions still need to be answered before it becomes clear where UAS flights will fall within the spectrum of possible procedures and policies. The most important

question revolves around whether or not UASs will be mandated by the FAA to fly Visual Flight Rules (VFR) or allowed to fly solely based on its GPS and electronic navigation and not a pilot's direct vision. Given the credible current security risks that have been uncovered (Humphrey hacking a drone in July 2012), it would seem likely that the FAA would err on the safe side and require UAVs to fly with constant visual contact with the ground and/or important navigation reference points. If this is the case then the operators of UASs will not be forced to divert their attention from private curtilage because FAA rules will dictate continuous sensory visual cues from the ground, thus creating a higher likelihood of infringement on United States citizens' Fourth Amendment rights. If UAV operators are allowed to operate their vehicles solely by the guidance of satellite and ground communications, a UAV "will have the ability to 'power down' its visual surveillance sensors until it reaches its target area, whether it is to execute an aerial search on a private residence or evaluate a forest fire" (Troy 2009, 12). Even if they must fly VFR, widespread fear about an overzealous big brother may keep any photographic and video evidence obtained by a UAV out of the courtroom.

Privacy watchdogs like the American Civil Liberties Union and members of Congress have been sounding the alarm with the growing reality of a drone inundation above our skies. "Rep. Ted Poe, a Texas Republican and former judge, will introduce the 'Preserving American Privacy Act,' which sets strict limits on when, and for what purpose, law enforcement agencies and other entities can use unmanned aerial vehicles … The measure … would require judicial warrants before any agency could employ a drone. It also restricts the use of UAVs by any state or local entity 'except in connection with the investigation of a felony'"(Wolfgang 2012). Similar bills have been introduced by Rep. Austin Scott (R-Ga.), and Sen. Rand Paul (R-Ky.), both requiring warrants for almost all law enforcement operations, except the most imminently

dangerous or life threatening situations. Ultimately UAV privacy issues will be settled by how the Fourth Amendment is interpreted.

Regulatory Issues

The challenges described above – safety, security and privacy – comprise only part of the regulatory hurdles that faces the FAA. Despite growing attention and research, creating registration, enforcement and standard operating procedures to work with the complicated existing regulatory system is a daunting challenge. H.R. 658, officially titled the FAA Modernization and Reform Act of 2012, mandates the Federal Aviation Administration, operating under the Department of Transportation, to streamline liscensing and other programs, create efficiencies, establish rules for certification and operation of drones, improve aviation safety and capacity, and oversee total integration of drones in American airspace (H.R. 658). In performing its regulatory duties the bill sets forth a number of deadlines the FAA must meet:

- May 14, 2012 – Expedite the licensure of government drones. Sec. 334(c)(2)(C)
- Aug. 12, 2012 – Early integration of "safe" government and non-government drones. Sec. 333 (a)-(b)
- Nov. 10, 2012 – Guidance for government drones and development of comprehensive plan for non-government drones. Sec. 334(a)(1)-(4)
- Dec. 31, 2012 – Final standards for government drones. Sec. 334(b)
- Feb. 14, 2013 – Deadline for comprehensive non-government drone plan. Sec. 332(a)(5)
- Aug. 14, 2014 – Final rule for non-government drones and proposed rule to implement comprehensive plan. Sec. 332(b)(1)-(2)
- Sep. 30, 2015 – Integration of non-government drones. Sec. 332(a)(3)

- Dec. 14, 2015 – Final rule to implement the comprehensive plan. Sec. 332(b)(2)
- Dec. 31, 2015 – Final standards for government drones. Sec. 334(b) (Geiger 2012)

Currently, only operators with Special Airworthiness Certificates can operate drones in public airspace and the Certificates of Authorization (COA) are hard to come by. The list of approved operators includes all three military branches and the Marines, DARPA, the departments of Homeland Security, Energy, Agriculture, Interior and Justice, the FBI and NOAA (National Oceanic and Atmospheric Administration) (FAA 2012). The list also includes local law enforcement agencies in Alabama, Arkansas, Colorado, Florida, Kansas, Minnesota, Texas, Utah and Washington, including the major cities of Arlington, Houston, Miami and Seattle. A wide range of research universities have been granted COAs, including Cornell, Georgia Tech, Kansas State, Mississippi State, Ohio, Texas A&M, Texas State, Utah State and the Universities of Arizona, Colorado, Connecticut, Florida and Michigan among others (see Appendix I for full list). The amount of issued licenses are far fewer than those who desire them, given the complex technical, operational and legal issues involved in integrating unmanned craft into the National Airspace System.

Even the existing COAs are questionable in their safety and regulatory scrutiny. Title 14 of the Federal Code of Regulations establishes the "rules of the road" for aircraft operating over U.S. skies. If these regulations were applied to UAVs, "the FAA has acknowledged 'there would be no UAV flights in civil airspace' if it applied existing detect, 'see-and-avoid' requirements strictly or vigorously" (Ravich 2010). Despite the host of on-board sensors and cameras, the lack of situational awareness mentioned earlier must meet the minimal safety standards of manned craft before UASs expand from their limited research and law enforcement allowance to widespread use. As discussed earlier, see-and-avoid ability is crucial to full UAS integration in

our skies, a feat yet to be accomplished, which has driven the FAA, through its COA authorization process, to implement a set of principles that may provide safe airways given the small number of licensed craft. But this process is not replicable for broad use. COA approval is limited to public entities like local law enforcement and state universities and is granted after the following three principles have been established:

- The COA authorizes an operator to use defined airspace and includes special provisions unique to the proposed operation. For instance, a COA may include a requirement to operate only under Visual Flight Rules (VFR) and/or only during daylight hours. Most COAs are issued for a specified time period (up to one year, in most cases).
- Most COAs require coordination with an appropriate air traffic control facility and may require the UAS to have a transponder to operate in certain types of airspace.
- Due to the inability of UAS to comply with "see and avoid" rules as manned aircraft operations do, a visual observer or an accompanying "chase" aircraft must maintain visual contact with the UAS. (UAS Fact Sheet n.d.)

The FAA issued 146 COAs in 2009 and 298 in 2010, more than doubling in one year. As of June 28, 2011, there were 251 active COAs, 90 different proponents and 77 different aircraft types (UAS Fact Sheet n.d.). As perhaps the least complicated classification of UASs, regulations for small UASs (sUAS) are currently being drafted, but the Notice of Proposed Rulemaking (NPRM) has been delayed more than a year because new provisions of H.R. 658 presumably created the DOT's explanation for delay: "unanticipated issues requiring further analysis" (Department of Transportation 2012). The FAA is working "with the Aviation Rulemaking Committee (ARC) comprised of industry, associations, and other government

agencies … (in creating) regulations to facilitate: certification of pilots; registration of aircraft; approval of sUAS (small unmanned aircraft systems) operations when required; and define sUAS operational limits, best practices, and regulatory approach for all sUAS" (FAA Aerospace 2011). It is likely that the FAA will work with the ARC in a similar manner to meet the 2015 deadlines established by H.R. 658.

Recommendations

Consistent with the typical rule making process of executive departments and agencies, it is important for the FAA to work closely with the relevant stakeholders – primarily industry leaders, public associations, law enforcement agencies and existing COA operators. The proposed rules for all types of UASs, whether corporate or public, small or large, are as of yet unavailable to the public. In considering the various regulatory schemes, the FAA must consider three essential questions:

- How will UASs handle communication, command, and control?
- How will UASs "sense and avoid" other aircraft? (UAS Fact Sheet n.d.)
- How UAS regulation will ensure the privacy rights of individuals?

The FAA must address these three main concerns before safe integration can occur. The complexity involved in answering these questions, accomplishing these actions and the aggressive timetable outlined by the FAA Modernization and Reform Act of 2012 creates significant challenges that must be overcome.

Without the significant progress of the last two decades, mostly due to advancing technology, unmanned aerial systems would not be on the cusp of entering the national airspace for routine use. However, the major issues examined above must be resolved before this can take place. DeGarmo (2004) recommends 10 actions be taken to achieve the goal of safe integration,

all of which require direct action by the FAA and cooperation from affected parties. Routine UAV operation will occur when we:

(1) Agree upon a concept of operations for UAV flights in civil airspace;

(2) Develop a classification scheme and definitions for UAVs as they relate to operations in civil airspace;

(3) Establish regulations for UAV system certification, flight operations, and ground controller qualifications;

(4) Develop effective technologies and procedures to prevent collisions of UAVs with other aircraft, the ground, or other obstacles;

(5) Institute security controls and approvals for UAV operations;

(6) Develop and implement communications solutions for UAV systems;

(7) Develop an aeronautical data exchange, processing, and synchronization network that accounts for unique UAV requirements;

(8) Internationally harmonize UAV regulations, certification standards, and operational procedures;

(9) Ensure interoperability with the air traffic system and assess potential impacts on the air traffic system and its regulatory and operational environment;

(10) Gain public acceptance and actively communicate with all potentially affected parties.

While DeGarmo created this checklist for integration in 2004, all of his outlined objectives continue to be among the important benchmarks to safe UAV flight as 2015 approaches. Harley Geiger, a writer for the Center for Democracy and Technology, recently

made another set of suggestions to ensure the transparency of domestic drone use. He recommends that all applicants for drone licenses should describe:

> 1) the purpose for which the drone will be used and the circumstances under which its use will be authorized and by whom, 2) the specific kinds information the drone will collect about individuals, 3) the anticipated uses and disclosures of that information, 4) the possible impact on individuals' privacy, 5) the specific steps the applicant will take to mitigate the impact on individuals' privacy, such as protections against unauthorized disclosure, 6) the individual responsible for safe and appropriate use of the drone, and 7) an individual point of contact for citizen complaints … The FAA should make all approved licenses, with the associated privacy statement of the drone operator, available online to the public in a searchable format. This requirement may have an exception for national security, but not for law enforcement. (Geiger 2011)

DeGarmo and Geiger make compelling recommendations to address the issues analyzed in this paper. Similar to their suggestions, this paper recommends the following actions be taken toward successful integration:

1) Conduct further research on traffic avoidance devices in order to find the most cost-effective method of lowering the probability of mid-air collisions.
2) Develop new technology that will make virtual cockpits more realistic by providing additional sensory cues that will add to a UAS operator's ability to control the vehicle safely.
3) Develop minimum standards for operator training, focusing on proficiency in

controlling the unmanned craft and interacting with other aircraft in the national airspace.

4) Increase investments in upgrading the NextGen Air Traffic Control System.
5) Work with other nations and international non-governmental organizations to develop uniform operational procedures that cross all country's borders.
6) Conduct more detailed analysis on UAS accident rate and safety performance to establish a baseline for improvement and insurance rates.
7) Research and implement new security technologies for civilian GPS to eliminate the possibility of GPS spoofing.
8) Protect UAS operational frequencies, common data links and video data links through implementation of spectrum management, electromagnetic hardening or counter-jamming technologies.
9) Facilitate UAS transparency by creating national and state databases of UASs including operators, the purpose of operation, flight information and statistics, security policies in place by the operator, contact and complaint information and other relevant disclosure information.
10) Draft legislation outlawing widespread general surveillance and requiring warrants for all surveillance except for emergency or national security purposes which would still be subject to retroactive judicial review.
11) Develop federal privacy guidelines for UAS operation that states, local agencies and private operators will model their privacy regulations on.
12) Realize that the FAA's expertise is aeronautical and relegate the authority of drafting privacy guidelines to the Departments of Homeland Security or Justice, which have

significant expertise in public safety, Fourth Amendment and privacy issues.

13) Support inter-departmental cooperation between the FAA, DHS, DOJ, DOT and other involved agencies to develop comprehensive regulations according to the mandate of the FAA Modernization and Reform Act of 2012.

Conclusion

Many complex issues surround the integration of unmanned aerial systems into the national airspace and all require significant research and regulatory efforts to meet minimum standards of safety, security and privacy.

To ensure operational safety, technological innovations must enable a UAS's operator to detect other aircraft to avoid midair collisions within the current and next generation air traffic control systems. The lack of standard training procedures requires regulatory attention to guarantee operators are competent and international regulations must be uniform to encourage UAS expansion.

To guarantee the security of unmanned aerial systems, exploitable weaknesses in civilian GPS technology and operational frequencies must be eliminated through the introduction of new or existing technologies in the most cost-effective manner.

The potential for Fourth Amendment privacy violations and the need to develop comprehensive privacy policies must be addressed to protect United States' citizens from unrestricted law enforcement and surveillance activity.

This paper reviews a host of the different challenges facing the FAA's efforts to adopt safety regulations enabling the integration of UAS into U.S. Skies. The Government Accountability Office summarized the current state of affairs excellently:

Routine UAS access to the national airspace system poses a variety of

> technological, regulatory, workload, and coordination challenges. Technological challenges include developing a capability for UASs to detect, sense, and avoid other aircraft; addressing communications and physical security vulnerabilities; improving UAS reliability; and improving human factors considerations in UAS design. A lack of regulations for UASs limits their operations and leads to a lack of airspace for UAS testing and evaluation and a lack of data that would aid in setting standards. Increased workload would stem from FAA's expectation of increased demand for UAS operations in the national airspace system without a regulatory framework in place. In addition, coordination of efforts is lacking among diverse federal agencies as well as academia and the private sector in moving UASs toward meeting the safety requirements of the national airspace system. (GAO 08-511)

While technology has catalyzed the aircraft industry allowing UAVs to be developed into operable machines, it will be human ingenuity and determination from federal regulatory agencies, primarily the FAA, which will ultimately facilitate UAV integration into America's navigable airspace.

Appendix I: Current Certificates of Authorization (COA)

U.S. Air Force
Arlington, Texas Police Department
U.S. Army
CAL FIRE (California Department of Forestry and Fire Protection)
City of Herington, Kansas
City of Houston, Texas Police Department
City of North Little Rock, Arkansas Police Department
Cornell University (Ithaca, New York)
DARPA (Defense Advanced Research Projects Agency)
DHS (Department of Homeland Security) / CBP (Customs and Border Protection)
DHS (Department of Homeland Security) / Science and Technology
DOE (Department of Energy) - Idaho National Laboratory
DOE (Department of Energy) - National Energy Technology Laboratory
Department of Agriculture - U.S. Forest Service
Department of Agriculture - U.S. Forest Service
Department of Agriculture - Agricultural Research Service
Department of Agriculture - Agricultural Research Service
Department of the Interior - National Business Center/Aviation Management Directorate (NBC/AMD)
DOJ (Department of Justice) - Queen Anne's County, Maryland Office of the Sheriff
Eastern Gateway Community College (Steubenville, Ohio)
FBI (Federal Bureau of Investigation)
Gadsden, Alabama Police Department
Georgia Tech Police Department, Office of Emergency Preparedness (Atlanta, Georgia)
Georgia Tech Research Institute (Smyrna, Georgia)
Hays County, Texas Emergency Service Office
Kansas State University (Manhattan, Kansas)
Mesa County, Colorado Sheriff's Office
Miami- Dade Police Department
Middle Tennessee State University (Murfreesboro, Tennessee)
Mississippi Department of Marine Resources (Biloxi, Mississippi)
Mississippi State University
Montgomery County, Texas Sheriff's Office
NASA (National Aeronautics and Space Administration)
U.S. Navy
New Mexico Tech (Socorro, New Mexico)
New Mexico State University Physical Sciences Laboratory (NMSUPSL) (Las Cruces, New Mexico)
Nicholls State University (Thibodaux, Louisiana)
NOAA (National Oceanic and Atmospheric Administration)
Ogden, Utah Police Department
Ohio University (Athens, Ohio)
Orange County, Florida Sheriff's Office
Otter Tail County, Minnesota

Polk County, Florida Sheriff's Office
Seattle, Washington Police Department
Texas A&M University Corpus Christi
Texas A&M University - TEES (Texas Engineering Experiment Station) (College Station, Texas)
Texas Department of Public Safety (Austin, Texas)
Texas State University (San Marcos, Texas)
University of Alaska Fairbanks
University of Arizona (Tucson, Arizona)
University of Colorado (Boulder, Colorado)
University of Connecticut (Storrs, Connecticut)
University of Florida (Gainesville, Florida)
University of Michigan (Ann Arbor, Michigan)
University of North Dakota (Grand Forks, North Dakota)
University of Wisconsin (Madison, Wisconsin)
USMC (United States Marine Corps)
Utah State University (Logan, Utah)
Virginia Commonwealth University (Richmond, Virginia)
Virginia Polytechnic Institute and State University (Blacksburg, Virginia)
Washington State Department of Transportation (Lacey, Washington)

Source: COA Sponsor List (accessed July 2012), available at
http://www.faa.gov/about/initiatives/uas/media/COA_Sponsor_List_042412.pdf

Appendix II: Selected Unmanned Aerial Vehicle Information

UAV	First Flight	Wingspan (Ft./In.)	Length (Ft./In.)	Gross (lb.)	Payload (lb.)	Max Speed (kt)	Ceiling (ft.)	Endurance (h)	Cost (U.S.$)*
		"							
Kettering Bug	1918[1]	15' 0"[1]	12' 6"[1]	530[1]	180[1]	100[1]	12,000[1]	1[1]	$3,600[1]
Messenger	1920[1]	20' 0"[1]	17' 9"[1]	862[1]	150[1]	84[1]	--	<2[1]	$38,000[1]
V-1	1944[2]	17' 8" [2]	27' 1"[2]	5,023[2]	2100[2]	325[2]	--	--	--
AQM-34 Lightning Bug	1964[3]	13' 0"[3]	29' 0"[3]	3,200[3]	--	560[3]	50,000[3]		$215,000[3]
Pioneer	1985[4]	16' 11"[4]	14' 0"[4]	450[4]	58[4]	177[4]	15,000[4]	5[4]	$850,000[5]
AeroVironment Helios	1999[1]	247' 0"[1]	12' 0"[1]	2,048[1]	726[1]	22 - 140[1]	90,000[1]	2[1]	--
MQ-9 Predator B	2007[6]	66' 0"[6]	36' 0"[6]	4,900[6]	3,750[6]	200[6]	50,000[6]	24[6]	$13.7[6]**
IAI Heron	1994[7]	54' 6"[7]	27' 11"[7]	2,535[7]	550[7]	70[7]	30,000[7]	>36[8]	$10[8]**
Northrup Grumman Global Hawk	1998[1]	116' 2"[1]	44' 5"[1]	25,600[1]	1,960[1]	345[1]	66,000[1]	42[8]	$68[8]**
SkySeer	1996[10]	6' 6"[9]	--	4[9]	--	24[9]	--	0.84 [9]	25,000[10]

In 2000 USD - *
In Millions USD - **

1 - Newcombe, Lawrence. Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles.
2 - http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=510
3 - http://www.hill.af.mil/library/factsheets/factsheet_print.asp?fsID=5796&page=1
4 - http://www.designation-systems.net/dusrm/app2/q-2.html
5 - http://airandspace.si.edu/collections/artifact.cfm?id=A20000794000
6 - http://www.af.mil/information/factsheets/factsheet.asp?id=6405
7 - http://www.mindef.gov.sg/imindef/news_and_events/nr/2011/mar/02mar11_nr3/02mar11_speech/02mar11_fs1.html
8 - http://www.isr.umd.edu/~austin/enes489p/projects2011a/BorderSecurity-Air-Team-FinalReport.pdf
9 - http://www.octatron.com/brochures/brochure-SkySeer.pdf
10 - http://news.cnet.com/2300-11394_3-6085259-2.html

Works Referenced

Bennett, Brian. 2012. "Police departments wait for FAA clearance to fly drones," *Los Angeles Times*, April 29. Accessed July 1, 2012. http://articles.latimes.com/2012/apr/29/nation/la-na-drone-faa-20120430.

Billingsley, T.B. 2006. "Safety Analysis of TCAS on Global Hawk Using Airspace Encounter Models," S.M. Thesis, MIT, Cambridge, Mass.

Bowes, Peter. 2006. "High hopes for drone in LA skies." BBC News, June 6. Accessed July 1, 2012. http://news.bbc.co.uk/2/hi/americas/5051142.stm.

California v. Ciraolo, 476 U.S. 207 (1986). FindLaw: Cases and Codes. Accessed July 31, 2012, at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=476&invol=207.

Caumont, Andrea. 2005. "Start-Up." *Washington Post*, November 28. Accessed July 1, 2012. http://www.washingtonpost.com/wp-dyn/content/article/2005/11/27/AR2005112700739.html.

Cloud, David, Jeffery Fleishman, and Brian Bennett. 2011. "U.S. drone strike in Yemen kills U.S.-born Al Qaeda figure Awlaki." *Los Angeles Times*, October 1. Accessed July 1, 2012. http://articles.latimes.com/2011/oct/01/world/la-fg-awlaki-killed-20111001.

Cox, T. H., Nagy, C. J., Skoog, M. A., & Somers, I. A. 2004. "Civil UAV Capability Assessment." National Aeronautics and Space Administration.

Degarmo, M. T. 2004. "Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace." *MITRE, Center for Advanced Aviation System Development*. Accessed July 1, 2012, at http://www.mitre.org/work/tech_papers/tech_papers_04/04_1232/04_1232.pdf.

Department of Transportation. 2012 "Rulemaking Management System - Report on DOT Significant Rulemakings." Department of Transportation." Accessed July 1, 2012, at http://regs.dot.gov/rulemakings/201205/report.htm#6.

Dow Chemical Co. v. United States, 476 U.S. 227 (1986). FindLaw: Cases and Codes. Accessed July 31, 2012 at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=476&invol=227.

Federal Aviation Administration. n.d. "COA Sponsor List." Accessed July 1, 2012 at ww.faa.gov/about/initiatives/uas/media/COA_Sponsor_List_042412.

Federal Aviation Adminstration. n.d. "FAA Aerospace Forecast Fiscal Years 2011–2031 Unmanned Aircraft." Accessed July 1, 2012, at http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2011-2031/media/Unmanned%20Aircraft%20Systems.pdf.

Federal Aviation Adminstration. n.d. "UAS Fact Sheet." Accessed July 1, 2012, at

www.faa.gov/about/initiatives/uas/media/uas_fact_sheet.pdf.

Geiger, Harley. 2012. “Drone Countdown.” Center for Democracy and Technology, March 27. Accessed July 1, 2012. https://www.cdt.org/blogs/harley-geiger/2703drone-countdown (accessed July 1, 2012).

Geiger, Harley. 2011. “The Drones are Coming.” Center for Democracy and Technology, December 21.Accessed July 1, 2012. https://www.cdt.org/blogs/harley-geiger/2112drones-are-coming (accessed July 1, 2012).

Gleason, J., Nefian, A., Bouyssounousse, X., Fong, T. and Bebis, G. 2011. “Vehicle detection from aerial imagery.” IEEE International Conference on Robotics and Automation, Shanghai,China.

Haddal, Chad, and Jeremiah Gertler. 2010. “Homeland Security: Unmanned Aerial Vehicles and Border Surveillance.” Congressional Research Service, Washington, DC.

Healey, Anthony, D. Horner, S. Kragelund, B. Wring, and A. Monnarez. 2007. “Collaborative Unmanned Systems for Maritime and Port Security Operations.” *Control Applications in Marine Systems* 7 (2007): 1. Accessed July 1, 2012, at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484372.

Humphrey, Todd. 2012. “Domestic Drone Overight; Committee: House Homeland Security; Subcommittee; Oversight, Investigations, and Management.” *Power Engineering*. Accessed July 1, 2012, at http://www.power-eng.com/news/2012/07/19/domestic-drone-oversight-nl-committee-house-homeland-security-nl-subcommittee-oversight-investigatio.html.

Ishutkina, Timothy Chan, Eric Feron. 2004. “Automation Technology for Off-Road Equipment.” Proceedings of the 7-8 October 2004 Conference: Kyoto, Japan.

Jensen, T. A., L. C. Zeller, and A. A. Apan. 2011. “The Use of an Unmanned Aerial Vehicle as a Remote Sensing Platform in Agriculture.” *Australian Journal Of Multi-Disciplinary Engineering* 8, no. 2: 139-146. Accessed July 1, 2012 on Academic Search Complete, EBSCO*host*.

Johnson, L., S. Dunagan, B. Lobitz, D. Sullivan, R. Slye, and S. Herwitz. 2003. “Collection of Ultra High Spatial and Spectral Resolution Image Data Over California Vineyards with a Small UAV.” International Symposium on Remote Sensing of the Environment. November 10 -14, 2003: Honolulu, HI.

Kalinowski, Nancy. 2010. “Testimony – Statement of Nancy Kalinowski.” Federal Aviation Administration. Accessed July 1, 2012, at http://www.faa.gov/news/testimony/news_story.cfm?newsId=11599.

Katz v. United States, 389 U.S. 347 (1967). FindLaw: Cases and Codes. Accessed July 1, 2012 at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=389&invol=347.

Keller, John. 2011. “U.S. Defense Spending for UAV Data Links and Ground-Control Stations Reached Billion-dollar Mark in 2010.” Military & Aerospace Electronics. Accessed July 1, 2012, at

http://www.militaryaerospace.com/articles/2011/10/u-s--defense-spending.html.

Koebler, Jason. 2012a. “First Man Arrested With Drone Evidence Vows to Fight Case.” *U.S. News & World Report*, April 9. Accessed August 4. http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case.

Koebler , Jason. 2012b. “Court Upholds Domestic Drone Use in Arrest of American Citizen.” *U.S. News & World Report*, August 2. Accessed August 4. http://www.usnews.com/news/articles/2012/08/02/court-upholds-domestic-drone-use-in-arrest-of-american-citizen.

Lucintel. 2011. “Growth Opportunity in Global UAV Market.” Accessed July 1, 2012, at www.lucintel.com/LucintelBrief/UAVMarketOpportunity.pdf.

M. Nas. 2008. “The Changing Face of the Interface: An Overview of UAS Control Issues and Controller Certification,” Unmanned Aircraft Technology Applications Research (UATAR) Working Group 27, 2008. Accessed July 1, 2012, at http://uatar.com/UAS%20Control%20Issues%20-%20UATAR%20%282%29.pdf.

McCarley J.S. and Wickens C.D. 2005. “Human Factors Concerns in UAV flight.” Institute of Aviation, University of Illinois. Accessed July 31, 2012, at www.hf.faa.gov/docs/508/docs/uavFY04Planrpt.pdf.

Moire. 2004. “Cost & Business Model Analysis for Civilian UAV Missions.” Accessed July 1, 2012, at http://bit.ly/10GBX9V.

New America Foundation. 2012. “The Year of the Drone | Counterterrorism Strategy Initiative.” Accessed July 1, 2012, at http://counterterrorism.newamerica.net/drones.

Nonami, Kenzo. “Prospect and Recent Research & Development for Civil Use Autonomous Unmanned Aircraft as UAV and MAV.” *Journal of System Design and Dynamics* vol. 1, no. 2 (2007): 120-128.

Oliver v. United States, 466 U.S. 170 (1984). FindLaw: Cases and Codes. Accessed July 31, 2012, at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=466&invol=170.

Padgett, Tim. 2009. “Using Drones in the Drug War.” *Time*, June 8. Accessed July 1, 2012. http://www.time.com/time/nation/article/0,8599,1903305,00.html.

PR Newswire. 2011. “Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012...” Accessed July 01, 2012 at http://www.prnewswire.com/news-releases/teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast-147008115.html.

Rapp, Geoffrey C. 2010. “Unmanned Aerial Exposure: Civil Liability Concerns Arising From Domestic Law Enforcement Employment of Unmanned Aerial Systems.” *North Dakota Law Review* vol. 85, no. 3: 623-648. Accessed July 1, 2012 on Academic Search Complete, EBSCO*host*.

Ravich, Timothy M. 2009. “The Integration of Unmanned Aerial Vehicles into the National Airspace.”

North Dakota Law Review 85, no. 3: 597-622. Accessed July 1, 2012 at Academic Search Complete, EBSCO*host*.

Roberts, Troy. 2009. "On the Radar: Government Unmanned Aerial Vehicles and Their Effect on Public Privacy Interests from Fourth Amendment Jurisprudence and Legislative Policy Perspectives." *Jurimetrics: The Journal Of Law, Science & Technology* 49, no. 4: 491-518. Accessed July 1, 2012, on Academic Search Complete, EBSCO*host*.

Shane A. Dougherty. 2002. "An Examination of Latency and Degradation Issues in Unmanned Combat Aerial Vehicle Environments." Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base.

Smith v. Maryland, 442 U.S. 735 (1979). FindLaw: Cases and Codes. Accessed July 1, 2012, at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=442&invol=735.

U.S. Congress. House. *FAA Modernization and Reform Act of 2012*. 112th Cong., 1st sess., H.R. 658. *Congressional Record*, January 18, 2011: H230 – 304.

UAV Collaborative. n.d. "UAV Applications: Fire Management - Project Overview." Accessed July 1, 2012 at http://www.uav-applications.org/projects/fire_1.html.

UAV MarketsSpace Consulting. n.d. "UAV Agriculture and Wildlife Management." Accessed July 1, 2012, at http://www.uavm.com/uavapplications/agriculturalwildlife.html.

United States Coast Guard. 2012. "USCG: Unmanned Aircraft System." Accessed July 1, 2012, at http://www.uscg.mil/acquisition/uas/default.asp.

United States v. Dunn, 480 U.S. 294 (1987). FindLaw: Cases and Codes. Accessed July 31, 2012, at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=480&invol=294.

Vacek, Joseph J. 2009. "Big Brother Will Soon Be Watching- Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement.." *North Dakota Law Review* 85, no. 3: 673-692. Accessed July 1, 2012, on Academic Search Complete, EBSCO*host* .

Warwick, Graham. 2012. "Civil UAVs Need GPS Anti-Spoofing, But Who Pays?" *Aviation Week*, July 19. Accessed July 21, 2012 at http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3A4861b58f-7472-47a7-8da7-8bb968fc3af3.

Weibel, R. & Hansman, R. 2005. "Safety Considerations for Operation of Unmanned Aerial Vehicles in the National Airspace System." Massachusetts Institute of Technology. Accessed July 1, 2012, at http://dspace.mit.edu/handle/1721.1/34912

Wolfgang, Ben. 2012. "Bill Would Clip Wings of Private Drone Use." *Washington Times*, July 20. Accessed July 31. www.washingtontimes.com/news/2012/jul/20/congress-steps-efforts-regulate-

drones/.

Yochim, J.A. 2001. “The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack.” M.M.A.S. Thesis, Fort Leavenworth, Kansas.

Yoo, John. 2011. “Assassination or Targeted Killings After 9/11.” *New York Law School Law Review* vol. 56, no. 1: 57-79. Accessed July 31, 2012, on Academic Search Complete, EBSCO*host*.