8-2013

Privacy and Unmanned Aerial Systems Integration in the National Aerospace System: Navigating Fourth Amendment Concerns

Dennis Vincenzi
Embry-Riddle Aeronautical University, vincenzd@erau.edu

David Ison
Embry-Riddle Aeronautical University, isond46@erau.edu

Dahai Liu
Embry-Riddle Aeronautical University, liu89b@erau.edu

PRIVACY AND UNMANNED AERIAL SYSTEMS INTEGRATION IN THE NATIONAL AIRSPACE SYSTEM: NAVIGATING FOURTH AMENDMENT CONCERNS

Dennis Vincenzi,[*] David Ison,[†] and Dahai Liu[‡]

A variety of challenges to the successful assimilation of UASs into the National Airspace System (NAS) currently exist. Technical issues and human factors related hurdles have brought forth a range of research efforts to help to mitigate or resolve these challenges. Regulations and legislation play a significant role in controlling or restricting the use of UASs in the NAS. Currently there appears to be a contraposition of sentiment between the Federal Aviation Administration and Congress on the inclusion of UASs in the NAS. Congress has called for the adoption of UAS operations in the NAS by 2015 yet the FAA has placed an assortment of restrictions and obstacles on the certification and use of UASs which severely inhibit research and development activities. Yet another setback has recently surfaced when the FAA suspended its selection process for UAS test sites due to privacy concerns. This new obstacle has the potential to further delay UAS integration. The privacy debate is inherent to American society. So important is the issue that it is covered in the Fourth Amendment of the U. S. Constitution. Public outcry concerning unwarranted or unknown observation is nothing new. With the advent of new surveillance technologies and techniques, concern that they may be used in violation of personal rights and protections has grown. Examples include wiretapping, electronic surveillance, video monitoring, and other types of law enforcement and related agency activities. This study identified themes among the dissent for such technologies as well as for UAS integration. Further, commonalities and occurrences in previous privacy-related confrontations were characterized in order to serve as a guide for efforts to resolve the UAS privacy quandary.

INTRODUCTION

It is foreseeable that the next generation of the flight will contain a great emphasis on Unmanned Aerial Systems (UASs). In today's environment, these systems are primarily operated by the military. UASs have been saving money, time and most importantly

[*] Chair, Department of Undergraduate Studies, Assistant Professor of Aeronautics, College of Aeronautics, Embry-Riddle Aeronautical University Worldwide, dennis.vincenzi@erau.edu
[†] Chair, Master of Aeronautical Science Program, Assistant Professor of Aeronautics, College of Aeronautics, Embry-Riddle Aeronautical University Worldwide david.ison@erau.edu
[‡] Associate Professor, Department of Human Factors and Systems, Embry-Riddle Aeronautical University Daytona Beach, dahai.liu@erau.edu

lives by stealthily and fearlessly penetrating enemy defenses, performing overt and covert surveillance, and in some cases, executing successful missile strikes on enemy targets behind enemy lines. Although the current applications are primarily limited to military operations, it is expected that in the near future, these applications could extend to a wide variety of other types of civilian services including search and rescue operations, weather research, homeland security operations, law enforcement operations, crop dusting, and oil pipeline inspection. Soon UASs will be participating in "aerial photography, surveying land and crops, and monitoring forest fires and environmental conditions" to name a few.

Congressional mandate for UAS integration and operation

One of the strategic objectives for FAA's NextGen initiative is to "make the national airspace system (NAS) scalable and flexible enough to incorporate various and new types of aircraft", including unmanned aircraft. The FAA is currently working on defining acceptable UAS performance standards and procedures to mitigate existing restrictions associated with UAS operations. The wide spread interest in the UAS arena is quickly increasing within the aviation community; the task of integrating UAS into the NAS has resulted in much attention and the creation of many dilemmas for the various different groups of stakeholders and researchers. Nevertheless, there are many critical issues that need to be addressed before a safe and acceptable integration of UAS into the NAS can take place, including technical issues, Human Factors issues, and ethical issues.

Among these factors, government regulation and legislation play a significant role in restricting the use of UAS in the NAS. According to the FAA Modernization and Reform Act of 2012, the bill provides $63.4 billion to fund the agency through 2015, including approximately $11 billion towards the FAA's proposed Next Generation ("NextGen") air traffic control system. It is also the first FAA funding bill to discuss integration of UASs into the NAS. Title III, Subtitle B states, among other things, that the FAA will have until September 30, 2015 to open the NAS to civil and commercial UAS aircraft. This Congressional mandate requires the FAA to work on a roadmap and plan to issue licensees to domestic entities to operate in areas that were previously only reserved for manned aircraft. As for the FAA, there are many hurdles to overcome to achieve this objective. Some of these hurdles include: [1]

- Ground control station issues/operator issues - these issues revolve around the question of how many operators should be present to control the UAS.
- UAS operations certification and UAS operator selection: what attributes/skills are necessary for operators to possess?
- Validation of the sense-and-avoid technology: what are acceptable industrial standard for those sense-and avoid technologies?
- UAS call signs: how to design the call signs for location and mission.
- UAS communication with ATC: how to establish a standard for UAS and ATC communication for safety and security.

Public concerns and outcries for protection of privacy

While these are the most commonly studied factors for the integration of UAS into the NAS, another setback has recently emerged as the FAA suspended its selection process

of UAS test sites due to concerns from the public over privacy issues. This right is recognized by the U.S. Supreme Court as protecting a general right to privacy. As for the use of UAS, the U.S. Supreme Court has held that individuals do not generally have Fourth Amendment rights with respect to aerial surveillance because of "the ability that anyone might have to observe what could be viewed from the air." There are more and more public concerns about the increasing use of UAS in the open airspace, despite the fact that most of the operations are government related and legal. For example, a recent protest led by the American Civil Liberty Union (ACLU) in Seattle, Washington resulted in the Seattle Police Department ending UAV operations for the city as concerns were raised involving invasion of privacy issues. In many states, legislators have voiced their concerns for the potential for privacy invasion posed by the wide use of UASs, worried about the personal information that could be collected by these small size drones. These and other examples have illustrated the growing concerns of the U.S. public as the use and potential abuse of UAS within the borders of the United States becomes more and more of a reality.

Civil rights such as privacy have been a major cause of concern for almost every government and commercial system put into use, and it is a critical issue that the UAS community must face and ethically resolve before considering the agenda of integrating UAS into NAS. As the ACLU has pointed out, "we need a system of rules to ensure that Americans can enjoy the benefits of this technology without bringing our country a large step closer to a "surveillance society" in which every move is monitored, tracked, recorded, and scrutinized by the authorities. An outline of protections that would protect Americans' privacy in the coming world of UAS" is in demand. [2] Without this outline of protections to safeguard Americans' privacy, public acceptance of UAS technology operating within the borders of the United States will be difficult to achieve.

REVIEW OF LITERATURE

Privacy

Brief background on the Fourth Amendment of the U.S. Constitution

For centuries, the U.S. citizens have enjoyed the protection of specific rights provided by the United States Constitution. Of particular concern today is the potential erosion of those protections afforded by the Fourth Amendment concerning the right of privacy and protection from unwarranted search and seizure. In the United States, the Fourth Amendment to the U.S. Constitution states *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."* The concept of protection of an individual's right to privacy is not outdated or obsolete by any means. The Fourth Amendment is as important and valid today as the day it was conceived and written into the Bill of Rights that was drafted by the first Congress on September 25, 1789, over 222 years ago.[3] The problem is that the technology being employed did not exist 222 years ago, and the framers of the Bill of Rights never envisioned this technology or how its capabilities could be used against individuals. The Fourth Amendment was designed and worded within the context of technology and capabilities in existence in the late 1789, not 2012. The issues at the center of the UAS

privacy debate revolve around: 1) the technology being used, 2) the capabilities of that new technology, 3) the manner in which that technology is being used, 4) the reason it is being used, and 5) the environment in which the technology is being used.

The concerns for privacy by U.S. citizens dates back to the American Revolution when representatives of the British government abused the "Writ of Assistance", which was a type of general search warrant used without cause, justification or concern for the rights or privacy of the individual. Today, in order to be able to enter and search an individual's home, the law enforcement agency must appear before a court of law and present probable cause as to why a legal search warrant should be issued, and name specific people and items of interest which are believed to be present and related to the specific investigation under consideration.

Interestingly enough, UAS technology being proposed for commercial use is not being questioned nearly as much as when the discussion turns to UAS technology being used by local, state, and federal law enforcement agencies.[4] A recent June 2012 poll conducted by Monmouth University reported that 42 percent of those sampled were very concerned about their own privacy if U.S. law enforcement started using UASs with high tech cameras, while 15 percent said they were not at all concerned. However, the same poll reported that of those sampled, 80 percent said they supported the use of UAS for search and rescue missions while 67 percent said they oppose the use of UAS to issue speeding tickets.[5]

The use of UAS technology and the environment in which they operate causes a great deal of confusion in terms of what is legal and what is illegal. For example, does a law enforcement officer (UAS operator) need probable cause to operate a UAS with a high resolution camera over an individual's home and fenced in yard? If they see something illegal during that flight, do they now have the right to enter a home or property to perform a search? These are questions that will probably be answered in the near future on a case by case basis as they occur in society.

Legislation

The most notable event in recent history that has contributed to the expansion of government powers has been the coordinated terrorist attack against the United States on September 11, 2001. Citing the need to increase the ability of the U.S. Government law enforcement and intelligence communities to be able to collect information that may help prevent future terrorist attacks, and thereby better protect the public, the USA PATRIOT Act of 2001 was introduced and signed into law by Congress and then President Bush. Many people favored this expansion of power by the Federal Government, but some saw it as a necessary evil that had great potential to erode the protections afforded law abiding citizens under the Fourth Amendment of the U.S. Constitution.

But the real resistance to the potential erosion of the Fourth Amendment came years later with the advent of UAS technology and the obvious surveillance capabilities this technology possessed. Other acts of congress began to be introduced to reinforce the various protections provided under the Fourth Amendment such as the Preserving Freedom from Unwarranted Surveillance Act of 2012, the Preserving American Privacy Act of 2012, and the Farmer's Privacy Act of 2012. The concern for invasion of privacy and

general abuse of power on the part of State and Federal law enforcement agencies along with enhanced technologies and increased surveillance capabilities seems to have sparked a real effort on the part of the public, the ACLU, and some politicians to reinforce Fourth Amendment protections and counter the potential abuse of technology presented by UAS surveillance capabilities.

USA PATRIOT Act of 2001

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was signed into law by President George W. Bush on October 26, 2001.[6] The act was a response to the terrorist attacks of September 11 which significantly weakened or removed restrictions on law enforcement agencies ability to gather intelligence within the United States against suspected terrorists. The immediate reaction to the USA PATRIOT Act of 2001 was overwhelmingly positive and supportive. It passed in the Senate by a vote of 98 – 1 and in the Hours of Representatives by a vote of 357 – 66.[7] Clearly, the American people and government of the United States was focused on taking steps to ensure that events similar to the September 11 attacks would not happen again. Additionally, the U.S. Government needed to reassure the American people that everything was under control and their government was taking positive steps to ensure their safety.

Embedded within the USA PATRIOT Act were 10 sections, Title I – X, which greatly enhanced the power and authority of law enforcement and intelligence agencies throughout the country. Without going into extreme detail on each section, the 10 sections are listed below:[8]

- Title I: Enhancing Domestic Security Against Terrorism
- Title II: Enhanced Surveillance Procedures
- Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001
- Title IV: Protecting the Border
- Title V: Removing Obstacles to Investigating Terrorism
- Title VI: Providing for Victims of Terrorism, Public Safety Officers, and Their Families
- Title VII: Increased Information Sharing for Critical Infrastructure Protection
- Title VIII: Strengthening the Criminal Laws Against Terrorism
- Title IX: Improved Intelligence
- Title X: Miscellaneous

All of the 10 titles included in the USA PATRIOT Act of 2001 are administrative and/or supportive of enhancing anti-terrorist initiatives to one degree or another. Title III, for example, deals with providing the resources and tools needed to identify, track,

and freeze money laundering and financial activities that are linked to the funding of terrorist organizations and/or terrorist activities. Title IV deals with taking the steps necessary to protect and secure the borders of the United States. Title IV does not address actual securing of open borders to prevent illegal crossing of the border into the United States, but rather deals with the denial of admission, verification of immigrant status, custody of aliens involved in terrorism, and eventual deportation or removal of the individual from the United States. Title VI deals with provisions for providing donations, payment, and support to victims of terrorism including the general public, public safety officers, and their families. Titles I, VII, VIII, IX, and X involve similar administrative and/or supportive guidance, but do not necessarily directly impact privacy or have any direct impact on the protections afforded by the Fourth Amendment.

Title II, however, potentially expands the powers of the Federal Government in ways that can easily undermine the Fourth Amendment protections if interpreted or implemented improperly or over-zealously by law enforcement agencies and the intelligence communities of the United States. Title II discusses enhanced surveillance procedures and specifically enumerates powers listed below:[7]

- Section 206: Allows for roving wiretaps under the Foreign Intelligence Surveillance Act, which allows the issuance of a court order the government to employ electronic surveillance of a foreign power or agent of a foreign power.
- Section 209: Allows law enforcement to seize voice mail messages pursuant to a warrant.
- Section 210: Allows law enforcement to subpoena additional subscriber records from service providers such as "records of sessions and durations" and "means and source of payment."
- Section 215: Allows the Director of the Federal Bureau of Investigation "access to certain business records for foreign intelligence and international terrorism investigations" where such investigation is to be "conducted under guidelines approved by the Attorney General."
- Section 216: Allows a Pen Trap, a device that records the numbers dialed but not the content of the conversation, to be applied to internet dialing and email.
- Section 220: Allows for "Nation Wide Service of Search Warrant for Electronic Evidence."

Clearly, on the surface, no one would object to "enhanced surveillance procedures" to help ensure the safety of the American people. However, recent news events have shown that these "enhanced surveillance procedures" can be interpreted very broadly and used to research and investigate data pertaining to all Americans, not just "foreign powers or agents of a foreign power." The recent National Security Agency (NSA) phone records scandal used portions of the USA PATRIOT Act of 2001 which references the Foreign Intelligence Surveillance Act to obtain a court order allowing collection of data from phone records from all Verizon customers (foreign and domestic) for the purpose of metadata analysis of information pertaining to those records including what phone num-

ber was called, what time the call was made, and duration of the call. In theory, the court order was obtained to research and investigate potential links between foreign entities, known terrorist entities and individuals, and suspected terrorist entities and individuals. In reality, this revelation has led to a renewed debate over the legality and policy merits of broad and indiscriminate government surveillance of Americans under the guise of national security.[9]

It is difficult to be certain as to the legality of this action since both the details of the program and legal rulings on it are classified as secret. But civil liberties groups argue the program exceeds the powers Congress has granted to the executive branch, and that such a broad surveillance program is inconsistent with the Fourth Amendment.[9]

The program appears to be partly based on Section 215 of the Patriot Act, which allows the government to obtain business records that are relevant to an ongoing terrorism investigation. That's a pretty permissive standard, but the Electronic Frontier Foundation argues that Congress intended to authorize information requests relevant to a specific terrorism investigation. Demanding the phone records of every person in the United States seems inconsistent with that requirement since it is highly unlikely that ALL Americans are terrorists.[9]

H.R. 5925 - Preserving Freedom from Unwarranted Surveillance Act of 2012

Oddly enough, critics of the potential erosion of Fourth Amendment protections from legislation such as the USA PATRIOT Act of 2001 were fairly quiet until the realization that electronic and physical surveillance was more feasible than ever before. With the advent of sophisticated surveillance equipment and the capability to deploy that equipment virtually anywhere, anytime in a covert manner (UASs performing surveillance silently from height of hundreds or thousands of feet in the air), concern began to grow on a national level.

One piece of legislation introduced on June 7, 2012 was H.R. 5925, the "Preserving Freedom from Unwarranted Surveillance Act of 2012." The purpose of this bill was to "*protect individual privacy against unwarranted governmental intrusion through the use of unmanned aerial vehicles commonly called drones and for other purposes.*" The Preserving Freedom from Unwarranted Surveillance Act of 2012 is a simple 3 page bill that reinforces the Fourth Amendment as specifically related to the use of "drones" or UASs involved in surveillance operations on U.S. Citizens. Section 2, Prohibited Use of Drones states, "*Except as provided in Section 3, a person or entity acting under the authority of the United States shall not use a drone to gather evidence or other information pertaining to criminal conduct or conduct in violation of a regulation except to the extent authorized in a warrant issued under the procedures described in the Federal Rules of Criminal Procedure.*" Section 3 lists exceptions to Section 2 such as patrol of borders, exigent circumstances (such as when law enforcement parties possess reasonable suspicion that swift action is needed to prevent loss of life or damage to property, or to forestall the imminent escape of a suspect or destruction of evidence) or to counter high risk of a terrorist attack by a specific individual or organization when credible intelligence exists.[10]

This bill was introduced on June 7, 2012 and was referred to committee (died) on June 7, 2012. It was reintroduced as H.R. 972 on March 05, 2013. H.R. 972 was referred to committee on May 22, 2013 and is currently pending committee review.[11] This current bill, according to GovTrack.us, has very little chance of getting past committee and very little chance of being enacted.

H.R. 6199 - Preserving American Privacy Act of 2012

The Preserving American Privacy Act of 2012 was very similar to the Preserving Freedom from Unwarranted Surveillance Act of 2012. The act states that drones cannot be used domestically by law enforcement or for surveillance of a U.S. national or real property owned by that national except pursuant to a warrant and in the investigation of a felony, and that information obtained in violation of that section using UASs may not be used in a criminal proceeding before a Federal court.[12]

This bill was introduced on July 25, 2012 and was referred to committee (died) on July 25, 2012. It was reintroduced as H.R. 637 on February 13, 2013. H.R. 637 was referred to committee on February 13, 2013 and is currently pending committee review.[13] This current bill, according to GovTrack.us, has approximately a 60% chance of getting past committee and approximately a 16% chance of being enacted.

So, it appears that although the American public and some American politicians are strongly supportive of the Fourth Amendment and acutely aware of the potential erosion of Fourth Amendment protections with the introduction and use of UAS technology, there is very little desire to actually pass any legislation reinforcing the Fourth Amendment through legislation at this time.

FAA Test Site Selection: Privacy Concerns

Included in the original wording of the FAA Modernization and Reform Act of 2012 is a requirement to develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the NAS, and that plan shall be implemented as soon as practicable, but not later than September 30, 2015. Also included in that same section is a requirement to establish 6 test ranges around the United States that will be used for research, development, and testing of UAS technologies, policies, procedures, and guidelines toward the safe integration of UAS into the NAS.

Shortly after the FAA Modernization and Reform Act of 2012 was signed into law, the FAA began to implement plans for test site selection and quickly ran into problems due to complaints received related to privacy issues and UAS use. In a letter addressed to the Congressional UAV Caucus, The FAA Acting Administrator, Michael Huerta, stated that "Our target was to have 6 test sites by the end of 2012. However, increasing the use of UAS in our airspace also raises privacy issues, and these issues will need to be addressed as unmanned aircraft are safely integrated." [14, 15]

The FAA and others have consistently stated and maintained that the FAA is charged with ensuring safe integration of UASs into the NAS, and that does not include catering to or developing regulation or guidelines related to privacy concerns. Critics of the FAAs decision to include privacy considerations into the test site criteria say that federal, state and local laws regarding the protection of an individual's right to privacy already exist,

including the Fourth Amendment. There are over 20 references to safety in Title III, Subsection B, but not one reference to privacy or privacy related concerns. [16] Critics of the FAAs decision to include privacy guidelines are mostly politicians who want to move the initiative along as quickly as possible in an attempt to secure a test site in their districts, or companies associated with the UAS industry in some way that see privacy as another hurdle or regulation that will slow things down causing more regulatory delays while less complicated, faster moving initiatives in other countries claim large shares of the global UAS market. However, the FAA maintains that the safe integration of UAS into the NAS must be thoughtful and well planned.

The FAA anticipates that test site operator privacy practices as discussed in their privacy policies will help inform the dialogue among policymakers, privacy advocates, and the industry regarding broader questions concerning the use of UAS technologies. The privacy requirements proposed here are specifically designed for the operation of the UAS Test Sites. They are not intended to pre-determine the long-term policy and regulatory framework under which commercial UASs would operate. Rather, they aim to assure maximum transparency of privacy policies associated with UAS test site operations in order to engage all stakeholders in discussion about which privacy issues are raised by UAS operations and how law, public policy, and the industry practices should respond to those issues in the long run.[17]

Case law and privacy

It is not uncommon for there to be confusion or uncertainty when actions or procedures conducted by individuals or government entities take place in untested circumstances. This is particularly an issue when new technologies are utilized in the conduct of criminal enforcement proceedings. Further, when the public learns of new and different ways in which they may be subject to observation, apprehension about general privacy typically arises. Because of the nascent nature of the use of UAS in the U.S., it is not surprising that privacy has become a considerable topic of concern among the public. Because UASs are a relatively new technology, it is impossible to assume that existing laws or interpretations thereof are adequate to manage their use in observation of the public and even more importantly, the ability to use evidence collected by UASs in criminal proceedings. At the same time, it is not fair for UAS opponents to claim that these devices be prohibited to be used in any way related to human surveillance. In the past, when new technologies or procedures have been introduced, namely in the collection of evidence by law enforcement or other government agencies, resolutions were only provided upon the testing of such in various court cases.

When these types of challenges occur, legal precedents are generated from the decisions. Stanford University defines a legal precedent as: "the decision of a court (or other adjudicative body) that has a special legal significance. That significance lies in the court's decision being regarded as having practical, and not merely theoretical, authority over the content of the law."[18] These decisions lay the ground for future cases heard on similar topics, as "if there are good reasons to believe that an earlier case was correctly decided, and if the facts in a later case are the same as those in the earlier case, then there are good reasons for believing that the same decision would be correct in the later

case."[18] Once precedents (case law) have been established, they begin to "have practical authority because they are regarded as partly constituting the law. Simplifying somewhat, the law is what the court stated it to be because the court stated it to be such."[18] Precedents are established by courts at various levels, both state and federal, but often pivotal cases end up in the U.S. Supreme Court. Such instances have the most wide ranging influence as they essentially supersede lower court decisions.

Many cases related to privacy as well as search and seizure have ended up in the Supreme Court. The resultant decisions have provided lower courts further guidance on how to handle the collection of evidence and to evaluate the legality thereof. In the past, any time law enforcement agencies have used novel techniques or technologies, they have seemingly ended up in a variety of level of appeals for consideration. Even if a precedent is established, it is not guaranteed that even minor changes in the way evidence may be collected will be considered to be under the same case law. In order for a precedent to apply, a court must decide if the present case is "identical" or "relatively the same" as the precedent case.[18] Even if a lower court decides that this is or is not the circumstance with the present challenge, it does not guarantee that this decision will not be challenged by a higher court. This cycle of case trials, evaluations, and reevaluations has become very common among the introduction of neophyte surveillance technologies and therefore should present no surprise that such is likely to occur in cases surrounding UASs. To understand how current surveillance precedents have been created, the road to present day case law must be examined.

General surveillance. The seminal document advocating for the privacy protection of citizens of the U.S. resides within the Fourth Amendment of the United States which states that "*the right of the people to be secure in their persons, houses, papers, and effects, against 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.*"[2] Much interpretation has been made by law enforcement, citizens, and most importantly, by courts, as to what is considered to be "unreasonable searches and seizures." Also, debate has centered on the term "probable cause" as well as just about every other statement within the amendment.[19] One of the earliest tests to the amendment itself was in the 1886 case of *Boyd v. United States*. In this case, the precedent to what is today considered reasonable in terms of search and seizure was partially developed. Being forced to produce business records was determined by the Supreme Court to be unreasonable, as other means of remedy were available.[18]

One of the principal guiding cases in terms of admissibility of evidence can be found in *Weeks v. United States*. In this case, search and seizure of the plaintiff was deemed to be unwarranted and thus illegal. The court decided that evidence that has been obtained illegally cannot be admitted. This case has provided individuals protection from questionable evidence collection techniques and technologies over the years and is still cited in cases concerning illegal gathering of evidence. [19] A formative case involving probable cause, *Brinegar v. United States*, established that police, given obvious indications that an individual is conducting a crime – in this case a heavily loaded vehicle being driven by a known and previously convicted liquor smuggler being operated in a suspicious location

– allows for the conduct of certain types of inquiry and search.[20] The courts have also advocated for the ability for police to search even without a warrant specific to such a search. In *United States v. Rabinowitz*, the court found that an arrest warrant in itself deemed probable cause and subsequent, reasonable search of premises within control of the accused could be conducted.[21]

Further honing what is deemed reasonable and probable cause, *Aguilar v. Texas* created the precedent that warrant requests must be based upon credible informants and/or reliable information. While definitions of these standards may vary, there must be more than hearsay or circumstantial evidence to provide the basis for search and seizure.[22] Police have also been limited in what they can provide as evidence based upon how and where such proof is collected. Without proper probable cause, evidence gathered incidental to an arrest may not be, in fact, admissible, as was the case in *Beck v. Ohio*.[23] Most subsequent case law, however, generally accepts evidence gathered post-arrest such as in "pat downs" and personal possession items. Also, if individuals consent to search, in most cases, the evidence found thereafter has been found to be admissible.[24]

Electronic monitoring and observation. With the advent of more sophisticated communications and the ability to "tap" or monitor them, the issue of privacy truly took on a different meaning. For instance, could talking on a telephone be considered to be a private transaction between speakers? In one of the first cases involving evidence collected via a wiretap of phone lines, *Olmstead v. United States*, the Supreme Court found that tapping was not considered a search or seizure. The justices noted what was lacking was a "material ingredient" meaning there was no physical removal or confiscation.[25] Probably one of the most important precedent cases related to privacy was *Katz v. United States* which challenged the aforementioned *Olmstead* case. In this dispute, the plaintiff stated that a conversation within a telephone booth should be considered private and immune from monitoring. The court favored the plaintiff yet they noted that places are not protected – instead personal privacy is what is to be considered. Thus even if an individual is visible in public, such as in a telephone booth, this does not mean that they lose all expectations of privacy. In fact, that is the nature of a telephone booth, so an individual can enter it to have a conversation that they reasonably expect to be private. Thus this case created the Harlan two-part test for determining privacy protection: 1. A person must have an actual expectation for privacy and 2. that this expectation is reasonable.[26]

Since *Katz*, reasonable expectation for privacy has been interpreted in a variety of ways. In general, when someone is in their residence, they are afforded the presumption of privacy. This apparently even applies to use of technologies that "pierce" into the privacy of one's home. In the case of *Kyllo v. United States*, Federal agents used thermal imaging devices to detect heat from growing lamps used to produce marijuana within the plaintiff's home. The Supreme Court determined that such evidence could not normally have been detected without a warranted search of the physical interior of the home. This case essentially placed a limit on the use of advanced technologies and monitoring devices on the ability to infiltrate instances deemed to be reasonably private. However, as the justices noted in this case, citing *Katz*, police are still able to use "plain sight" and other reasonable "senses" to procure evidence.[27] A case that precedes *Kyllo* exemplifies this extra "loophole" available to police – *United States v. Cusumano*. Similar to *Kyllo*, the

defendant's home was "searched" by a thermal device. The difference in this case was substantial other evidence was used to provide probable cause, such as power usage, admission of the defendant as to owning growing lamps, gardening supplies, payment of rent in cash, and the procurement of additional electrical supplies to the basement through the services of a professional electrician. The courts found that aside from the thermal evidence, other indications existed that were suspicious enough to merit closer scrutiny.[28] Whilst case law indicates that individuals should be immune from the use of advanced technologies to infiltrate the home, precedent does not support the notion that all parts of an individual's home or adjacent property are immune from observation.

Once law enforcement started to use aerial observation, several cases have been heard at the state and Federal Supreme Court levels to argue the admissibility of evidence garnered from such over-flights. *United States v. Hester* defined two terms of significance related to aerial surveillance: curtilage and open fields. Curtilage is defined as the areas adjacent to a home, such as a yard. Whilst curtilage is subject to privacy protection from a spectator walking on the ground if it is properly hidden, e.g. with a solid, high fence, it is not protected from incidental aerial observation from above.[29]

Several important precedents were established relating to privacy, curtilage, and observation techniques and technologies in *California v. Ciraolo*. In this case, a police helicopter, working on a tip, overflew the defendant's residence at 1,000 feet in navigable airspace. Even though the defendant had a ten-foot privacy fence, this observation was made from above in plain sight. Photographs were taken using a standard 35mm camera to document the growth of marijuana plants in the defendant's yard. The use of aerial surveillance to view illegal activities in plain sight using conventional technologies (i.e. those readily available to the public) was considered acceptable and the ruling against the defendant was upheld.[30] Similarly, in *Dow Chemical Company v. United States*, Environmental Protection Agency personnel used an aircraft to overfly a chemical plant, secured with fencing, utilizing mapping cameras to photograph the facility. Evidence from this flight was used for EPA enforcement purposes. Because the plant was considered "open fields," the aircraft was flown within navigable airspace, and utilized non-enhanced photographic means of data collection, the evidence collected on such a flight was deemed usable in court.[31] *Florida v. Riley* narrowed the concept of presumed privacy of a residence. During a flight at 400 feet, a police helicopter observed an opening in a greenhouse in an obscured backyard. Through this gap, marijuana was seen growing in the building. All observations were made with the naked eye. The Supreme Court found that this was not an illegal search in the scope of the law.[32] Also, precedent has determined that almost any actions in public places to be observable without a warrant. Even video observation is acceptable, as the crime deterrent brought forth by the installation of such cameras outweighed rights to privacy.[33]

Court decisions have created limitations to aerial surveillance, however. One such limitation was made apparent in *Colorado v. Pollock* in which it was determined that observation flights below reasonable navigational altitudes did, in fact, constitute an illegal search. The court noted that "rarely, if ever would ... normal air traffic in or near the defendant's residence be as low as 200 feet."[34] Thus there is a limit to how low or intrusive

aerial observations can take place. In a recent decision, however, a U.S. District Court found that the evidence collected from the installation of video cameras on private property by police was admissible.[35]

In general, precedent has also prohibited the use of "dragnet" type observation, i.e. prolonged, constant surveillance, except under the confines of a warrant. In both *United States v. Knotts* and *United States v. Karo*, the allowance for tracking of individuals was deemed permissible.[36, 37] These cases have also been cited to support GPS location of individuals as long as such is conducted with a warrant. In *Knotts*, Justice Rehnquist stated "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision. But the fact is that the reality hardly suggests abuse; if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Thus simply because a technology exists does not mean that there should be laws to control their uses – instead the resultant data that may be collected should be the subject of potential control or limitation.[36]

While this description of case law is not exhaustive, it does highlight the key cases related to current standards for privacy and surveillance. It is evident that there is a long and oft challenged line of cases that have taken place in order to form present day precedents. And due to the ever-changing legal landscape and contestations of the law, it is likely that UASs will provide fodder for further wranglings.

DISCUSSION

Potential application of case law

The concept of privacy and the legality of various types of surveillance have significant precedent cases to reference in future proceedings. Yet, even in light of current case law, it is apparent from the historical trend in such legal actions that precedent specific to UAS will likely need to be set. This is likely first to be challenged upon the premise that UAS surveillance is not "identical" or "relatively the same" as other types of observation. This test could theoretically go either way with the end result perhaps being specific to the individual case or situation. On one hand it could be argued that UASs do pose a unique threat to privacy, as alluded to in *Colorado v. Pollock*, for example their stealth nature, ability to maneuver into spaces and positions unable to be reached by manned aircraft, and capability to loiter for extended periods, thus requiring a distinctive evaluation by the court. Contrarily, it could be argued that UASs do not pose an idiosyncratic means of observation and as long as they adhere to current standards for aerial observation, no further manipulation of precedent would be required as was made clear by Justice Rehnquist in *Knotts*.

A decisive issue that will influence how UASs will be used in surveillance relates to the legality of the collection of evidence. As was set in *Weeks*, special care will need to be taken to insure that data collection by UAS conforms to the standards within all current precedent cases. This precaution is necessary to insure that evidence is not suppressed due to the conformance of the collection with previous cases. This may necessitate tests to probable cause and warrantless observation. It is certainly reasonable to be-

lieve that observations by UASs could in themselves provide probable cause, such as circumstances noted in *Brinegar* or *Ciraolo*, providing the proof necessary to allow for more intrusive means or even a warrant. Considering *Ciraolo* and *Dow Chemical Company*, warrantless surveillance could easily take place over residences, of curtilage, and of open fields which certainly may provide probable cause or even hard evidence for potential prosecution.

One potential sequence that could ensue, relying on concepts in the *Brinegar, Rabinowitz, Aguilar*, and *Beck* cases, is that UASs could be sent on a mission to observe, purposefully or not, a certain locale. During this surveillance a suspicious circumstance is observed giving probable cause. Depending upon the situation, this could be used to pull over a car or approach an individual for further questioning. If an arrest then takes place, all evidence collected at the point of arrest would likely be admissible. Alternatively, evidence from the observation could be used to generate a warrant query. Once the warrant is secured, most evidence would be accepted in court proceedings especially if following a subsequent arrest. It is therefore plausible that challenges will come to the ability of UASs to establish probable cause yet as long as these devices are operated within the confines of current case standards, it is likely that that such uses would be hard to challenge successfully.

Additional standards are likely to be considered applicable to UAS surveillance. One is the Harlan test for privacy. It seems that individuals inside their residence, a place of personal sanctity, should be safe from intrusive observation so visions of one opening their curtains to the sight of a quad-copter UAS hovering just outside is more fiction than fact. Yet individuals being in clear view either in curtilage or even in an open window may be subject to observation, as was the case in the "incidental" viewing of evidence in *Riley*. Additional challenge to what is considered to be an "expectation for privacy" may surface when UASs are used in and around a residence or other "private" structure.

Concerns about high tech surveillance systems that are readily available on UAS platforms being used in observation or collection of data/evidence also are unjustified. Current precedent seems to support protection from intrusive technologies such as thermal imaging, facial recognition, night vision, and other systems that are not typically available to the general public – the current accepted standard for such technologies.[X14X20] Although with the lowering costs of advanced imaging technologies, it is possible that one day in the near future the argument could be made that, say, night vision systems are within practical reach of an average individual, thus could become more likely to be admissible. Again, this will likely need to be hashed out in the court system. Further, it is conceivable that a naked-eye over-flight observation of suspicious activity could bring forth probable cause to pursue further action including the obtaining of a warrant for the use of advanced technologies which has typically held up to court inspection.

Lastly, the stealth and mobility of UASs will likely be limited by the standards in *Pollock, Riley, Ciraolo*, and *Dow Chemical Company.* In particular, the concept of reasonable expectation of overflight and navigable airspace will be critical to admissibility of collected evidence. It seems that an altitude of operation below 400 to 500 feet would be considered unacceptably intrusive. This would certainly limit the ability of the UAS, us-

ing only conventional visual cameras – at best with zoom capabilities – to closely observe or detect malicious activities or materials. Clearly public fears of UASs buzzing outside their bedroom windows again appear to be farfetched.

Forcing the hand – getting a case into court

It is apparent that new challenges must be made to UAS usage to clarify and solidify case law that may be applicable to such operations. Although there may be apprehension within UAS manufacturers, purchasers, and users about court challenges, it is actually in the best interest of all parties for such a "force of hand." With a challenge to the use of UAS will come clarification concerning what types of operations, technologies, and methods of surveillance will be tolerated by the courts. This is will give stakeholders solid ground on which to stand for future operations or allow for adjustments in the way such technologies are used. This is certainly better than the nebulous environment that exists today, pending approval of UAS use in domestic airspace. It may even be to the advantage of UAS stakeholders, particularly manufacturers, to see the use of UASs come before the courts. Why? Because it makes no sense to invest in something which may be illegal to use essentially making the device useless or the market for such extremely small. On the contrary, if UAS observation and technologies are upheld, it will open to the door to a broader audience of purchasers and make the job of salespersons significantly easier. Although challenges to UAS are already in the works, stakeholders should be open, if not pursue, the establishment of case law precedents.

CONCLUSION

Just as it was impossible for the framers of the U.S. Constitution to predict what technological development might cause sections of their document to become obsolete or meaningless, it is impossible for anyone today to envision what technological breakthrough may occur in the near future that may make these debates on privacy and UAS technology moot or obsolete. Some people feel that the technology used makes no difference and that existing laws, rules, and regulations that guard an individual's privacy are sufficient to handle any issue or challenge that may arise. Others believe that new technology and creative uses of that technology offer an opportunity or a gray area where the rules may be temporarily reinterpreted until they are challenged in court. Still others believe that new technology and new capabilities are a necessary step in updating current laws to make them less ambiguous and enhance protections at the same time.

Many laws are created based on the current state of technology, availability of that technology, and affordability of that technology. There is little debate surrounding the surveillance capabilities or potential erosion of Fourth Amendment protections when full size, manned helicopters are used by law enforcement agencies because they are known technology, their capabilities are a known quantity (at least for now), they are expensive to purchase, operate and maintain (not everyone can get one), and where they can fly is strictly regulated by the FAA and airspace regulations. UASs on the other hand are unknown quantities from almost every perspective. Their technology and current capabilities are known only to the military because they have been the primary user and develop-

er of UAS and UAS sensor technology to date, they are affordable and will become more affordable as the widespread use and demand increases, and where they can fly and operate is not strictly regulated by anyone at the current time.

Drones or UASs are nothing more than machines or tools to be used for a variety of purposes and in a variety of ways. As is often the case, the technology may not be the problem, but what people plan to do with that technology is what must be regulated. Careful and thoughtful development of new laws that consider the advanced capabilities and creative implementation of this new technology is one way to mitigate abuse and prevent erosion of Fourth Amendment rights and protections. Laws can be developed that consider a wide variety of situations and circumstances, but laws cannot be developed that cover every possible scenario.

Technologies such as the internet and cell phones have advanced at a far faster rate than can be reasonably regulated. As a result, much of the legislation regulating to these two areas was produced after the technology was available and already in use for many years.[38] With UAS technology, early consideration is being given to the potential uses and abuses of this technology in an effort to maximize legal commercialization of this technology while minimizing the potential abuse of this technology. This practice of early consideration coupled with thorough and thoughtful design of legislation should be encouraged and will result in the creation of a solid foundation for the future preservation of Fourth Amendment protections.

REFERENCES

[1] Stephen B. Hottman, Kari Sortland (2006), 6. UAV Operators, Other Airspace Users, and Regulators: Critical Components of an Uninhabited System, in Nancy J. Cooke, Heather L. Pringle, Harry K. Pedersen, Olena Connor (ed.) *Human Factors of Remotely Operated Vehicles (Advances in Human Performance and Cognitive Engineering Research, Volume 7)*, Emerald Group Publishing Limited, pp.71-88.

[2] Domestic Drones. http://www.aclu.org/blog/tag/domestic-drones

[3] Bill of Rights. http://www.archives.gov/exhibits/charters/bill_of_rights.html

[4] Thompson, R. M. *Drones in domestic surveillance operations: Fourth Amendment implications and legislative responses.* Washington, DC, Congressional Research Service, 2012.

[5] Monmouth University Poll, *"U.S. supports some domestic drone use, but public registers concern about own privacy."* (June 12, 2012).

[6] The USA Patriot Act: Preserving Life and Liberty. http://www.justice.gov/archive/ll/highlights.htm

[7] Horowitz, R. *Summary of Key Sections of the USA Patriot Act of 2001.* http://www.rhesq.com/Terrorism/Patriot_Act_Summary.pdf

[8] USA PATRIOT Act of 2001. Public Law 107-56. http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html

[9] Everything you need to know about the NSA's phone records scandal. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/06/everything-you-need-to-know-about-the-nsa-scandal/

[10] H.R. 5925 Preserving Freedom from Unwarranted Surveillance Act of 2012. http://www.govtrack.us/congress/bills/112/hr5925

[11] H.R. 972 Preserving Freedom from Unwarranted Surveillance Act of 2013. http://www.govtrack.us/congress/bills/113/hr972

[12] H.R. 6199 Preserving American Privacy Act of 2012. http://www.govtrack.us/congress/bills/112/hr6199

[13] H.R. 637 Preserving American Privacy Act of 2013. http://www.govtrack.us/congress/bills/113/hr637

[14] FAA Delays UAV Testing Site Selection "Indefinitely" http://www.acro-news.net/index.cfm?do=main.textpost&id=ac39756c-90a6-429c-915f-42acb2c76a94

[15] FAA Delays creating drone test sites due to privacy concerns. http://www.nextgov.com/emerging-tech/2012/11/faa-delays-creating-drone-test-sites-due-privacy-concerns/59845/

[16] Federal Aviation Administration Unmanned Aircraft system Test Site Program. http://mercatus.org/publication/federal-aviation-administration-unmanned-aircraft-system-test-site-program

[17] Unmanned Aircraft Systems. http://www.faa.gov/about/initiatives/uas

[18] Boyd v. United States, 116 U.S. 616 (1886).

[19] Weeks v. United States, 232 U.S. 383 (1914).

[20] Brinegar v. United States, 338 U.S. 160 (1949).

[21] United States v. Rabinovitz, 339 U.S. 56 (1950).

[22] Aguilar v. Texas, 378 U.S. 108 (1964).

[23] Beck v. Ohio, 379 U.S. 89,91 (1964).

[24] Schneckloth v. Bustamonte, 412 U.S. 218 (1973).

[25] Olmstead v. United States, 277 U.S. 438 (1928).

[26] Katz v. United States, 389 U.S. 347 (1967).

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

[28] United States v. Cusumano, 10 U.S. 94 (1996).

[29] United States v. Hester, 365 U.S 57 (1924).

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

[31] Dow Chemical Company v. United States, 476 U.S. 227 (1986).

[32] Florida v. Riley, 488 U.S. 445 (1989).

[33] Griswold v. Connecticut, 381 U.S. 479 (1965).

[34] Colorado v. Pollock, 796 P. 2d 63 (1990).

[35] United States v. Magana & Mendoza, (2012).

[36] United States v. Knotts, 460 U.S. 276 (1983).

[37] United States v. Karo, 468 U.S. 705 (1984).

[22] Aguilar v. Texas, 378 U.S. 108 (1964).

[23] Beck v. Ohio, 379 U.S. 89,91 (1964).

[24] Schneckloth v. Bustamonte, 412 U.S. 218 (1973).

[25] Olmstead v. United States, 277 U.S. 438 (1928).

[26] Katz v. United States, 389 U.S. 347 (1967).

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

[28] United States v. Cusumano, 10 U.S. 94 (1996).

[29] United States v. Hester, 365 U.S 57 (1924).

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

[31] Dow Chemical Company v. United States, 476 U.S. 227 (1986).

[32] Florida v. Riley, 488 U.S. 445 (1989).

[33] Griswold v. Connecticut, 381 U.S. 479 (1965).

[34] Colorado v. Pollock, 796 P. 2d 63 (1990).

[35] United States v. Magana & Mendoza, (2012).

[36] United States v. Knotts, 460 U.S. 276 (1983).

[37] United States v. Karo, 468 U.S. 705 (1984).

[38] Villasenor, John. Observations from Above: Unmanned Aircraft Systems and Privacy. (2013). http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_457_Villasenor.pdf