10/24/13 Task Force Meeting: Presentations and Public Testimony

<TARGET><BILL></BILL><SUBJECT>10-24-13 Task Force Meeting Presentations and Public Testimony</SUBJECT><COMM>JUNM28</COMM></TARGET>

Unmanned Aircraft Systems Legislative Task Force

October 24, 2013 Meeting at Anchorage LIO Room 220

Task Force Members:

- Representative Shelley Hughes, Co-Chair
- Senator Donny Olson, Co-Chair
- Ginger Blaisdell, Staff to Rep. Hughes
- David Scott, Staff to Senator Donny Olson
- McHugh Pierre, Department of Military and Veterans' Affairs
- Greg Walker, University of Alaska Fairbanks
- Ro Bailey, University of Alaska Fairbanks
- Lieutenant Steve Adams, Commissioner Designee, Department of Public Safety
- Steve Strait, Aviation Advisory Board, Governor's Office and DOT/PF
- Steve Colligan, Representative Member for the Academy of Model Aeronautics

Guest Attendee:

- Jay Skaggs, FAA
- Harry Kieling, Dept of InterioR

A G E N D A

8:30am Welcome and Introductions — Representative Shelley Hughes

Task Force responsibilities per HCR6

The duties of the task force shall include (1) reviewing regulations and guidance from the Federal Aviation Administration regarding unmanned aircraft systems; (2) providing written recommendations, together with suggested legislation, for a comprehensive state policy for unmanned aircraft that protects privacy and allows the use of unmanned aircraft systems for public and private applications; and (3) submitting, not later than January 15, 2014, an initial report to the legislature and, not later than July 1, 2014, submitting a final report to the legislature.

Brief Remarks About October 23rd Testimony

- **General Theme of Remarks**
- **Lessons Learned by Testifiers**
- **Continue to accept public testimony in writing**

8:35am **List of Documents Provided** **Ginger Blaisdell, staff**

1. **FAA Guidelines document N8900**
2. **Legal Services Memo**: Alaska Laws Protecting Privacy
3. **Observations from Above**: Unmanned Aircraft Systems and Privacy
4. **Alaska Law Review**, June 1995
5. **Aerospace States Association**: UAS Privacy Considerations and correspondence from ACLU, AK Department of Law, Airborne Law Enforcement Association, International Association of Chiefs of Police Aviation Committee, American Legislative Exchange Council, AUVSI, Electric Frontier Foundation, Electronic Privacy Information Center, Douglas Marshall, NACDL, and a sample bill.
6. **International Association of Chiefs of Police Aviation Committee**
7. **Academy of Model Aeronautics Policy**
8. **State of Texas Privacy Act**
9. **Homeland Security:** Privacy Impact Assessment for the Aircraft Systems

8:40am-10:00am **Overview of FAA Guidelines** **Greg Walker and Ro Bailey, UAF**

US DOT, FAA N8900.207
Unmanned Aircraft Systems (UAS) Operational Approval

10:00am-10:30am **Law Enforcement Review** **Lt Steve Adams, AK State Troopers**

International Association of Chiefs of Police Aviation Committee
Recommendations from experience in Alaska

As we go through these documents and listen to presentations, the task force may want to consider the legislative approach to the following topics:

Report/Bill

- Does the Task Force want to introduce a report separate from the introduction of a bill as requested in HCR6?
- What does the task force want in a report to the legislature?
- What kind of supporting documentation should be provided with the bill?

Legal Services Memo: Page 2
"The Court might find the use of a technology that exceeds human observational capacity the sort of intrusion that constitutes a search requiring a warrant or an accepted exception."
State of Texas Privacy Act: Page 1
What exceptions may need to be considered in legislation? Should the legislation prohibit uses and allow exceptions – OR – allow everything and specify prohibited uses?

Legal Services Memo: Page 4 and 5
"If the data is gathered by a government agency, it is a public record. However, AS 40.25.120 provides certain protections for private information." Inadvertent capture of evidence of illegal activity: "Use of inadvertently captured information in a criminal prosecution may depend on who captures the information, and whether the person whose actions have been captured has a reasonable expectation of privacy."
Under what circumstances would a court grant a search warrant to follow up on information inadvertently obtained, but not in "plain view?"

Observations from Above: Page 487-488
As technology continues to advance beyond 'normal' application of current laws, drafting new laws must adopt a balanced approach that recognizes the inherent difficulty in predicting the future.
How should Alaska law address law enforcement activities that might be considered 'uncommon practice' or 'routine' in reference to advanced technological capabilities? (such as thermal imaging)

Observations from Above: Page 495
"... But future (technological) developments will make long-term surveillance with UAS possible."
Should duration of flight hours be a consideration for exemptions of warrantless observations and intelligence collection or general flight use for any purpose?

Observations from Above: Page 503
"... in common law, a plaintiff generally must establish, at a minimum, that the intrusion was intentional and that it would be highly offensive to a reasonable person."
Do we need to consider a definition for "highly offensive to a reasonable person?"

Observations from Above: Page 508
Voluntary approaches of self-managed rules of UAS.
Do we want to adopt specific guidelines from the International Association of Chiefs of Police, AUVSI, Academy of Model Aeronautics, etc.? What if these guidelines make changes that are in conflict with Alaska Constitution or Alaska Law?

Observations from Above: Page 511
Suggestions for legislation:

- Consider the role that could be played by unintentionally captured images

- Legislation that would include a blanket prohibition on government use of private UAS data in criminal investigations would also be ill advised, as well as inconsistent with what routinely occurs in noninvasive settings.
- Any new legislation should recognize that images of public spaces from UAS will sometimes also include images of private spaces (nearby homes).
- State statute and scope of Federal Preemption: does not prevent state from passing any laws relating to how aircraft are flown.
- A state does not have the authority to enact UAS privacy laws that would decrease the safety of flight operations.

Miscellaneous comments from the public for the task force to consider:

1. Certification of Aircraft – who would certify, license, fee associated, "FAA is short on inspectors"
2. UAS pilot's license with differing levels of certification (hobbyist – commercial pilot plus UAS training hours)
3. Education provisions to train UAS Pilots
4. Specialized (high visibility) marking of UAS or lighting so that other aircraft can spot them
5. Insurance needs for private UAS operators
6. Who is responsible in educating the public
7. Disclaimer or disclosure for hobbyists when they purchase UAS
8. How to market Alaska as "Open for Business" for UAS operations
9. Public reporting requirements of UAS missions
10. Audits of UAS operators
11.

1:30pm – 4:30pm Public Testimony

Calls limited to 3 minutes each

4:30pm **Wrap Up** **Representative Hughes**

Ginger will summarize the documents discussed at this meeting and request a bill draft for our next meeting.

Task Force Timeline and Next Meeting Date/Time

Adjournment

FAA Guidelines for UAS

Alaska Legislative Task Force

10-24-13
FAA GUIDELINES
RO BAILEY
AK CTR. FOR
UA SYSTEMS

Ro Bailey

Deputy Director

Alaska Center for Unmanned Aircraft Systems Integration

(907) 455-2104

Review

- Current Regulations
  - Definitions & Exceptions
- Guidelines, Policy, & COAs
- 2012 FAA Reauthorization Act
- How is Privacy Protected?
- What's Needed to Fully Integrate UAS into the National Airspace System

The Governments Authority to Regulate UAS Flight Operations

- The Government obtains its authority to regulate the NAS through statutes enacted by Congress.
- Based on statutory authority, the FAA's responsibility is to implement regulations which carry out Congress's intent.
- 49 USC § 40103(b) states that "The FAA Administrator shall prescribe air traffic regulations regarding the flight of aircraft for:
  - (A) Navigating, protecting, and identifying aircraft;
  - (B) Protecting individuals and property on the ground;
  - (C) Using the navigable airspace efficiently; and
  - (D) Preventing collision between aircraft, between aircraft and land or water vehicles, and between aircraft and airborne objects."

Definitions

- NAS = National Airspace System
- UAS = Unmanned Aircraft System (FAA official term)
  - Unofficial terms include UAVs, RPAS, drones
    - UAV = Unmanned Aircraft or Aerial Vehicle
    - RPAS = Remotely Piloted Aircraft System
- RC aircraft = Remotely controlled aircraft, refers to model aircraft
- AMOC = Alternate Mode of Compliance
- SA or S&A = See and Avoid or Sense and Avoid

What is an Aircraft?

- 49 USC § 40102 defines an aircraft as "any contrivance intended, used, or designed to navigate, or fly in, the air."
  - UAS are categorized as aircraft

- Therefore, all statutes and regulations relating to "aircraft" include UAS
- However, some contrivances that fit the definition above are actually defined out...

Examples

Aircraft

- Cessna 172
- Boeing 787
- ScanEagle
- Scout

Not Aircraft

- Balloon
- Ultralight
- Model aircraft
- Light Sport Aircraft
- Kites

Public vs Civil Aircraft

- Congress further defined aircraft by distinguishing between "civil" and "public"
  - A "civil aircraft" is any aircraft except a "public aircraft"
  - A "public aircraft" includes:
    - An aircraft that is used only for Government purposes, or
    - An aircraft that is leased or owned by the Government
- FAA authority differs between civil & public aircraft

49 USCS §44711

- Prohibits a person from operating a "civil aircraft" without an airworthiness certificate.
- Prohibits a person from acting as an "airman with respect to a civil aircraft."
  - Does not regulate public aircraft users
  - Public users expected to establish & follow adequate airworthiness determinations & training—and assume the liability for operations
- All aircraft must comply with rules-of-the-road (FAR91)

FAA Modernization & Reform Act of 2012
Subtitle B--Unmanned Aircraft Systems

- Sec. 331. Definitions
  - (1) Arctic
  - (3) Permanent Areas
  - (4) "Public" UAS
  - (5) Sense & Avoid
  - (6) "Small" UAS
- Sec. 332. Integration of civil unmanned aircraft systems into national airspace system
  - Required Planning for Integration
  - Rulemaking
  - Pilot Projects
  - Expanding the use of UAS in the Arctic
- Sec. 333. Special rules for certain unmanned aircraft systems
  - General
  - UAS Assessments
  - Requirements for Safe Operation
- Sec. 334. Public unmanned aircraft systems.
  - Guidance
  - Standards for Operation and Certification
  - Agreements with Government Agencies
- Sec. 335. Safety studies. The FAA shall carry out all safety studies necessary to support the integration of unmanned aircraft systems into the national airspace system.
- Sec. 336. Special rule for model aircraft.
  - General
  - Statutory Construction
  - Model Aircraft Defined
- Sec. 901. Authorizations or Appropriations
  - (b)(15) UAS Research
- Sec. 903. Unmanned Aircraft Systems.
  - Sec. 913. Review of FAA's Aviation Safety-Related Research Programs
  - (15) Unmanned aircraft systems research.

FAA Modernization and Reform Act of 2012

SEC. 332. INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS INTO NATIONAL AIRSPACE SYSTEM

REQUIRED PLANNING FOR INTEGRATION

- COMPREHENSIVE PLAN—Not later than 270 days after enactment ... to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system.
  - The plan shall provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, but not later than September 30, 2015.
- REPORT TO CONGRESS—Not later than 1 year after the date of enactment ... a 5-year roadmap for the introduction of civil unmanned aircraft systems into the national airspace system

RULEMAKING

- Not later than 18 months ... a final rule on small unmanned aircraft

PILOT PROJECTS

- ESTABLISHMENT—Not later than 180 days after the date of enactment establish a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges.

Pilot Projects - continued

SEC. 332. INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS INTO NATIONAL AIRSPACE SYSTEM

TEST RANGE LOCATIONS—In determining the location of the 6 test ranges the Administrator shall—

(A) take into consideration geographic and climatic diversity;

(B) take into consideration the location of ground infrastructure and research needs; and

(C) consult with the National Aeronautics and Space Administration and the Department of Defense.

TEST RANGE OPERATION— operational not later than 180 days after the date on which the project is established.

Expanding Use of Unmanned Aircraft Systems in the Arctic

SEC 332 (d)

"…. the Secretary shall develop a plan and initiate a process to ….designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day for research and commercial purposes."

- "Arctic" means the United States zone of the Chukchi Sea, Beaufort Sea, and Bering Sea north of the Aleutian chain.
- Designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day for research and commercial purposes.
- Operations in these permanent areas shall include the development of processes to facilitate the safe operation of unmanned aircraft beyond line of sight.
- Such areas shall enable over-water flights from the surface to at least 2,000 feet in altitude, with ingress and egress routes from selected coastal launch sites.
- Approving the use of unmanned aircraft in the designated permanent areas in the Arctic without regard to whether an unmanned aircraft is used as a public aircraft, a civil aircraft, or a model aircraft.

Special Rules for Certain Unmanned Aircraft Systems

SEC 333 SPECIAL RULES FOR CERTAIN UNMANNED AIRCRAFT SYSTEMS.

IN GENERAL—not later than 180 days shall determine if certain unmanned aircraft may operate safely in the NAS before completion of the plan and rulemaking

ASSESSMENT OF UNMANNED AIRCRAFT SYSTEMS—the Secretary shall determine, at a minimum—

(1) which types of unmanned aircraft systems, if any, as a result of their size, weight, speed, operational capability, proximity to airports and populated areas, and operation within visual line of sight do not create a hazard to users of the national airspace system or the public or pose a threat to national security; and

(2) whether a certificate of waiver, certificate of authorization, or airworthiness certification is required for the operation of unmanned aircraft systems identified under paragraph (1).

REQUIREMENTS FOR SAFE OPERATION—If the Secretary determines under this section that certain unmanned aircraft systems may operate safely in the national airspace system, the Secretary shall establish requirements for the safe operation of such aircraft systems in the national airspace system.

Public Unmanned Aircraft Systems

SEC 334 PUBLIC UNMANNED AIRCRAFT SYSTEMS

GUIDANCE—Not later than 270 days after enactment, shall issue guidance regarding the operation of public unmanned aircraft systems to—

(1) expedite the issuance of a certificate of authorization process;

(2) provide for a collaborative process with public agencies to allow incremental expansion of access to the national airspace system as technology matures and the necessary safety analysis and data become available, and until standards are completed and technology issues are resolved;

(3) facilitate the capability of public agencies to develop and use test ranges, to test and operate unmanned aircraft systems; and

(4) provide guidance on a public entity's responsibility when operating an unmanned aircraft without a civil airworthiness certificate issued by the Administration.

STANDARDS FOR OPERATION AND CERTIFICATION—Not later than December 31, 2015, the Administrator shall develop and implement operational and certification requirements for the operation of public unmanned aircraft systems in the national airspace system.

Agreements with Government Agencies

SEC 334 (c)

IN GENERAL—Not later than 90 days after enactment, the Secretary shall enter into agreements to simplify the process for issuing certificates of waiver or authorization

CONTENTS—The agreements shall—

(A) with respect to an application

(i) provide for an expedited review of the application;

(ii) require a decision by the Administrator on approval or disapproval within 60 business days of the date of submission of the application; and

(iii) allow for an expedited appeal if the application is disapproved;

(B) allow for a one-time approval of similar operations

(C) allow a government public safety agency to operate unmanned aircraft weighing 4.4 pounds or less, if operated—

within the line of sight of the operator; less than 400 feet above the ground, during daylight conditions;, within Class G airspace; and outside of 5 statute miles from location with aviation activities.

Safety Studies

SEC. 335 SAFETY STUDIES

The Administrator shall carry out all safety studies necessary to support the integration of unmanned aircraft systems into the national airspace system.

Authorizations or Appropriations

SEC 901 Authorizations or Appropriations

AUTHORIZATIONS.—The following programs described in the research, engineering, and development account of the national aviation research plan required under section 44501(c) are authorized:

(12) Unmanned Aircraft Systems Research

Unmanned Aircraft Systems

SEC 903 UNMANNED AIRCRAFT SYSTEMS

RESEARCH INITIATIVE—

in conjunction with other Federal agencies, as appropriate, to develop technologies and methods to assess the risk of and prevent defects, failures, and malfunctions of products, parts, and processes for use in all classes of unmanned aircraft systems that could result in a catastrophic failure of the unmanned aircraft that would endanger other aircraft in the national airspace system."

SYSTEMS, PROCEDURES, FACILITIES, AND DEVICES—

to develop a better understanding of the relationship between human factors and unmanned aircraft system safety; and to develop dynamic simulation models for integrating all classes of unmanned aircraft systems into the national airspace system without any degradation of existing levels of safety for all national airspace system users."

Special Rule for Model Aircraft

SEC 336 SPECIAL RULE FOR MODEL AIRCRAFT

IN GENERAL—Notwithstanding any other provision of law...the Administrator may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft, if—

(1) the aircraft is flown strictly for hobby or recreational use;

(2) the aircraft is operated in accordance with a community based set of safety guidelines and within the programming of a nationwide community-based organization;

(3) the aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;

(4) the aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and

(5) when flown within 5 miles of an airport, ...without a mutually-agreed upon operating procedure with the airport operator or the airport air traffic control tower.

Models vs UAS

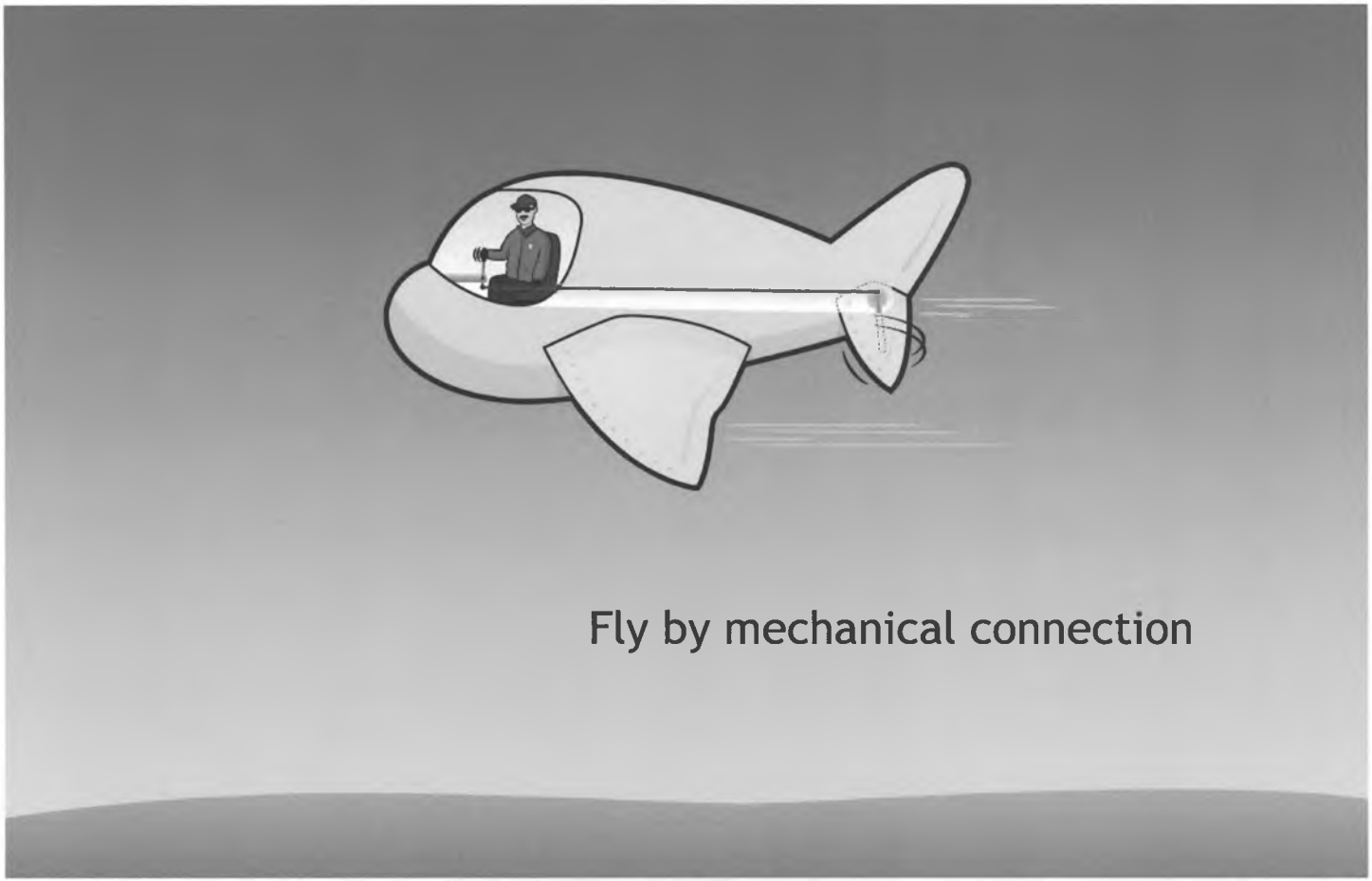
- The sole difference is how the equipment is used
  - Both may be hand controlled or autonomous
  - Both may carry complex payloads
  - Size and complexity vary in both
- A model, or hobbyist aircraft may only be used for non-business purposes
- The same equipment becomes a UAS if used for:
  - Paid services (surveying land for client)
  - Support your own business (photos for realtor)
  - Any activity that can be called "work"
- Governed by AC 91-57 published 6/9/1981 modified by 2012 reauthorization act

Pilot Licensing & Evaluation

14 CFR part 61

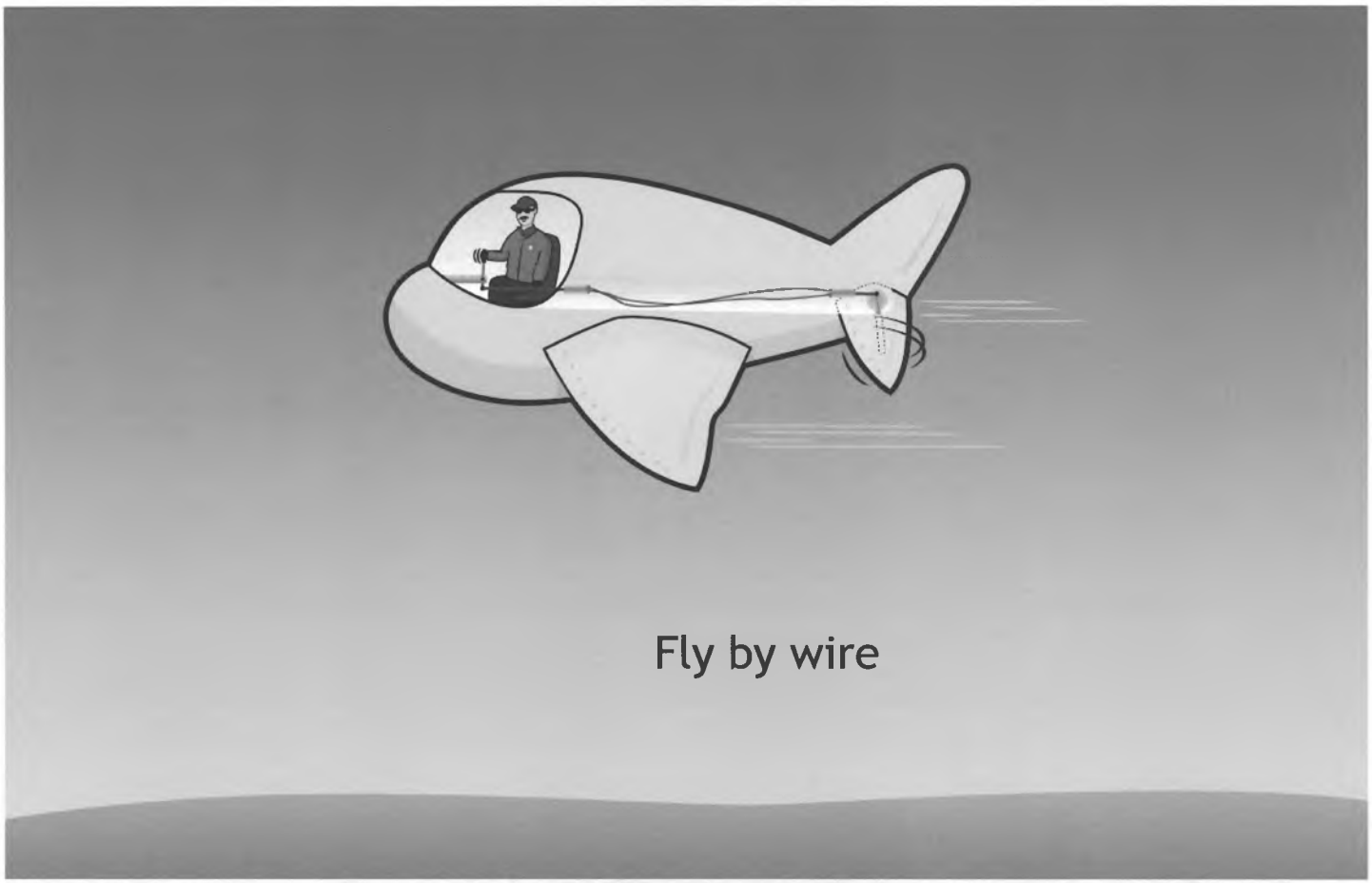
- Identifies applicability & requirements for eligibility, training, experience, currency, examination for all levels of pilots, instructors & examiners
- Part 67 identifies medical certificate requirements
- FAA policy 8900.227 provides interim requirements for UAS pilots, but no UAS-specific training or medical requirements have been incorporated into 14 CFR as yet

Manned vs Unmanned Control



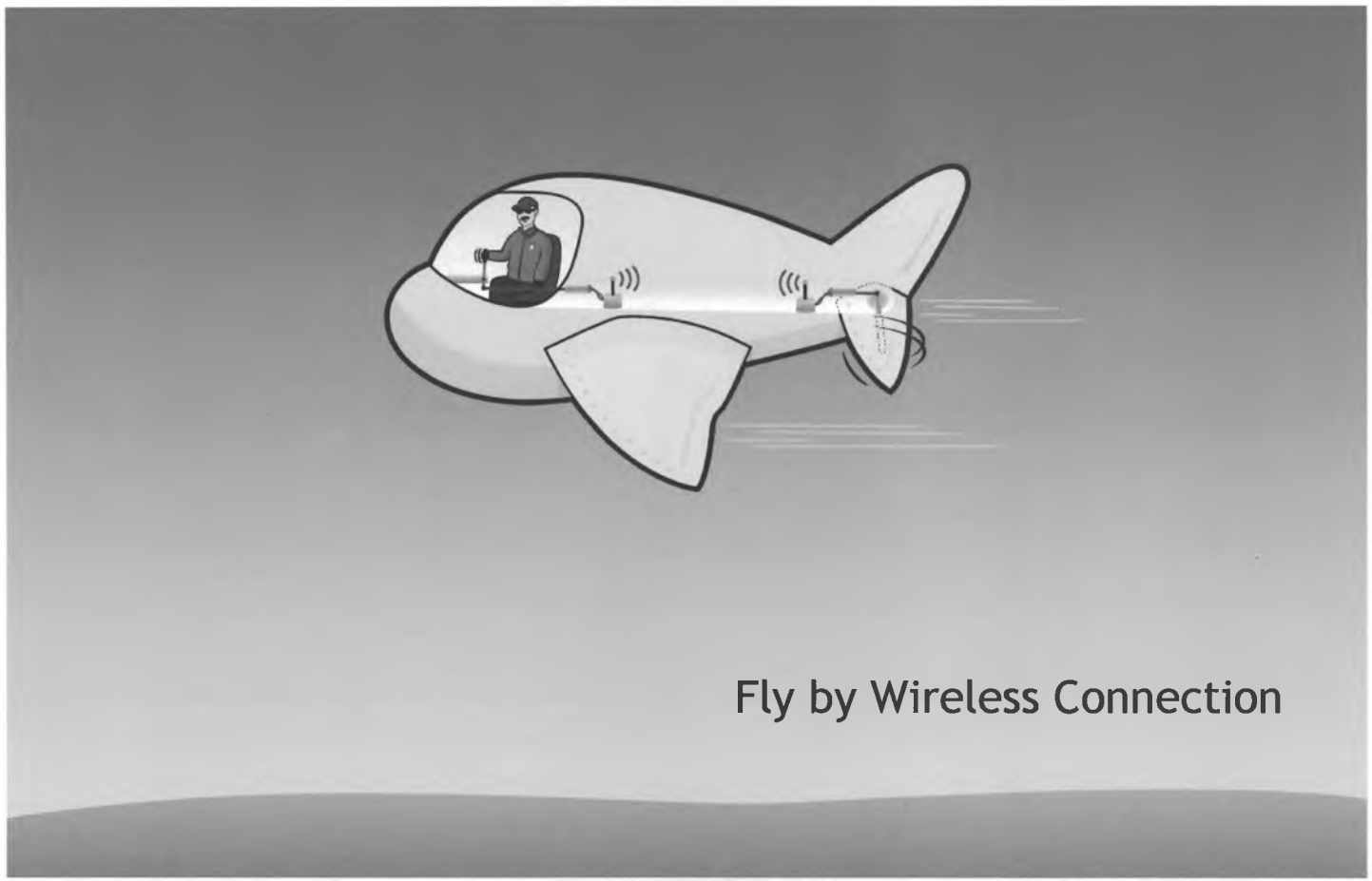
Fly by mechanical connection

Manned Control

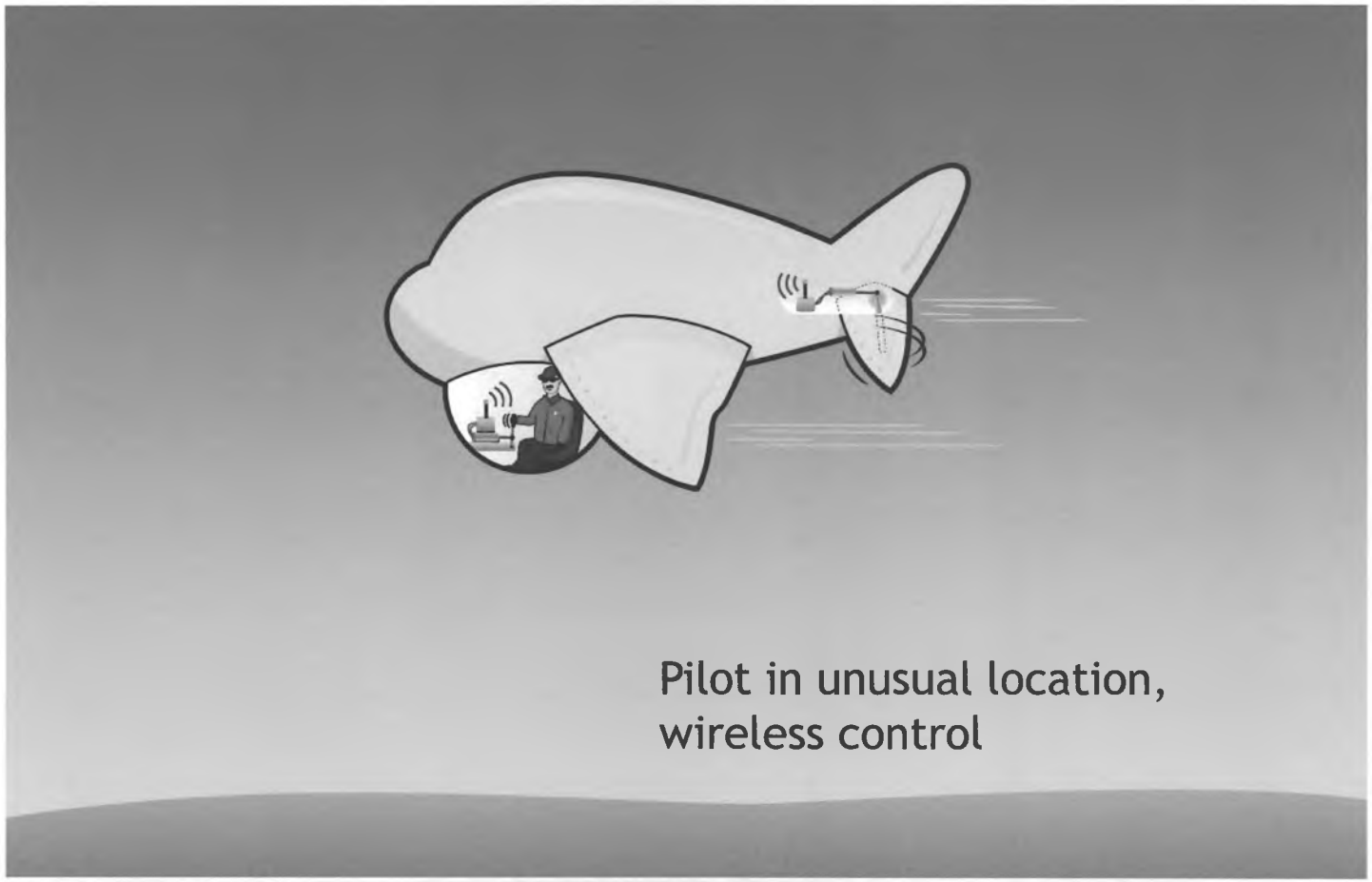


Fly by wire

Modern Manned Control



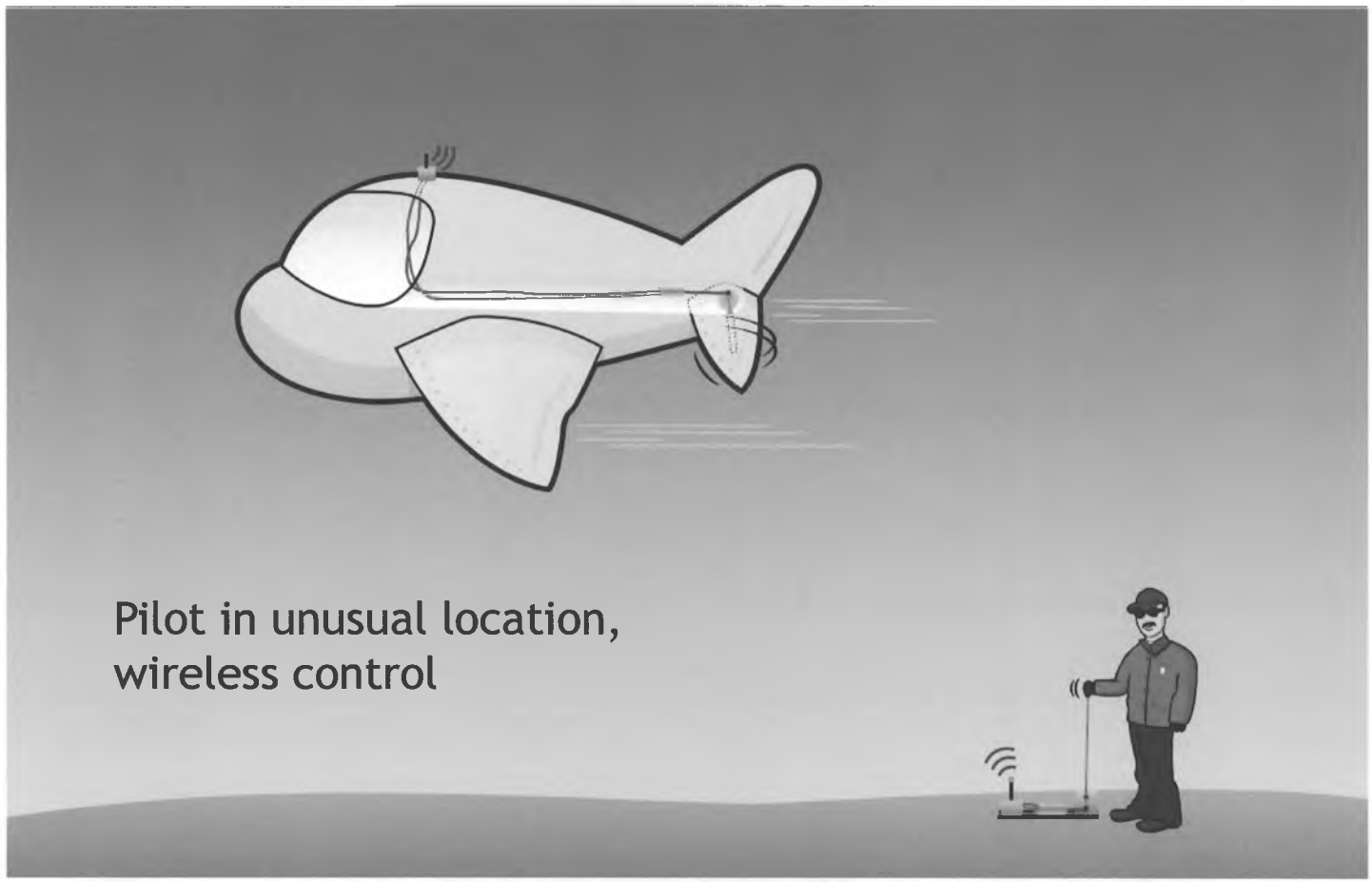
More Wireless Control



Pilot in unusual location,
wireless control

Unmanned Control

Beyond Line of Sight Becomes See & Avoid Issue



Challenges of See and Avoid for UAS

Issued for Part 91 Non-compliant Operations within the National Airspace.

These approvals are required due to the fact that unmanned aircraft (UA) are not compliant with various sections of Title 14 of the Code of Federal Regulations (14 CFR) and therefore, require an alternate means of compliance. *Most notably, the lack of an on-board pilot requires an alternate method of the "see-and-avoid"* provisions of 14 CFR 91.113, Right-of-Way Rules: Except Water Operations. - Interim Operational Approval Guidance 08-01

See and Avoid v. Sense and Avoid

- Alternate means of compliance must meet the reasonable standard of the eye of the onboard human pilot to "see and avoid" other objects.
- Bottom line is the pilot must make sure the airspace is clear.
- FAA approves alternative means of compliance for manned aircraft. Therefore "see and avoid" can be equated to "sense and avoid" which can be accomplished by technical means equal to or better than the human eye.
- Logic argues that the use of reliable primary radar, collision avoidance systems, or airspace studies showing no air traffic sufficiently demonstrate safe operations and comply with the spirit of CFR 91.113(b) and prior FAA decisions.

See and Avoid

The courts have ruled that CFR 91.113(b) requires "the reasonably prudent pilot need not be super-human in seeing and avoiding other aircraft, but he or she must scan the sky with such frequency and respond with such precision as is possible." Technology may assist the pilot, such as collision avoidance equipment or radar.

The FAA has acknowledged the following alternative means of compliance:

- In Class A (controlled) airspace the FAA authorizes Air Traffic Control (ATC) to provide separation guidance to aircraft (both manned and unmanned)
- The FAA approved use of primary radar to "sense" other aircraft
- FAA approves chase vehicles as acceptable replacement for an onboard pilot's eyes in which "eyes" are kept on the unmanned aircraft from another plane, a chase car, or a ground observer

Role of the Six Test Sites

- Assist FAA to resolve the issues preventing integration
  - Conduct safety studies
  - Develop potential policies, procedures
  - Establish their own training, certification, assess success, & report to FAA
  - Work toward standards for type certification, evaluate UAS offered by manufacturers
  - Propose changes/improvements to FAA regulations

Status of FAA Test Site

- Jan 2012: FAA Reauthorization Act directed FAA to select 6 Test Sites to research and test for safe integration of UAS into the national airspace
- Feb 14 2013: Solicitation was released
- Proposals final submittal was May 6
- Selection underway; rumors abound but no real news
- Selection targeted by FAA for Dec 31 2013
- Then Other Transactions Agreement negotiated
- Then 180 days to reach operational status

Pan Pacific UAS Test Range Complex

- UAF leads team for states of Alaska, Oregon, and Hawaii, plus 57 additional team members
  - Includes state agencies (DOT, DPS, Forestry of DNR, DHS&EM, National Guard)
  - Universities, EDCs, corporations, associations
- Fourteen ranges around the three states
  - Strong link with military ranges
  - Forging links with manned aviation safety specialists
- Key questions to answer:
  - Procedures to protect manned aviation
  - Policies to protect privacy
  - Technical testing to assure control, see & avoid, lost link procedures, airworthiness, etc

How is Privacy Protected?

- Intend to protect privacy so beneficial uses can be obtained
- Current statutory/case law strongly protects privacy while defining legal airborne activities (manned)
  - Unmanned a new technology, but subject to same restrictions
  - DHS & National Institute for Justice have taken on task of defining specific UAS privacy rules
  - FAA will incorporate into Test Site and future rules
  - DoD & Guard training on domestic privacy well underway

More on Privacy

- International Association of Chiefs of Police issued guidelines for law enforcement use of UAS
  - Provided to Task Force, available online
  - The essence:
    - Follow FAA rules
    - Use strict supervisory accountability
    - Get warrants if any possibility of use for surveillance or investigation
    - Notify locals of intent to fly over them
    - Delete recordings not authorized by warrant, training use, or as required by law

Where's the Gap?

- Gaps in privacy protection not yet apparent
- No incidents claiming UAS violated privacy so far
  - When it happens, propose letting the system work it
  - Existing law & prior manned case law likely adequate
  - Create law only to cover gaps discovered in practice, not in "what if" thinking

Summary

- Technology & FAA rules in flux
  - US behind other nations—could lose lead
  - Current rules restrictive, complex, limited to public entities
  - FAA compliance with 2012 Reauthorization Act driving toward UAS integration & comprehensive rules
- Alaska opportunities significant
  - Enhanced by directives in 2012 law


UAF
UNIVERSITY OF
ALASKA
FAIRBANKS
Questions?


UAF
UNIVERSITY OF
ALASKA
FAIRBANKS
Alaska Center for UAS Integration
Thanks for your time!

What Alaska Offers

- Vast open airspace with little traffic
- Wild, extreme, unpopulated, diverse terrain
- Access to large military ranges with data gathering ability
- History of pioneering aviation technology
- Culture of innovative use of aviation
- Close relationship with regional FAA
- Perhaps most important, willingness to be thoughtful and methodical in potential policy decisions
- Legislation setting Alaska airspace aside

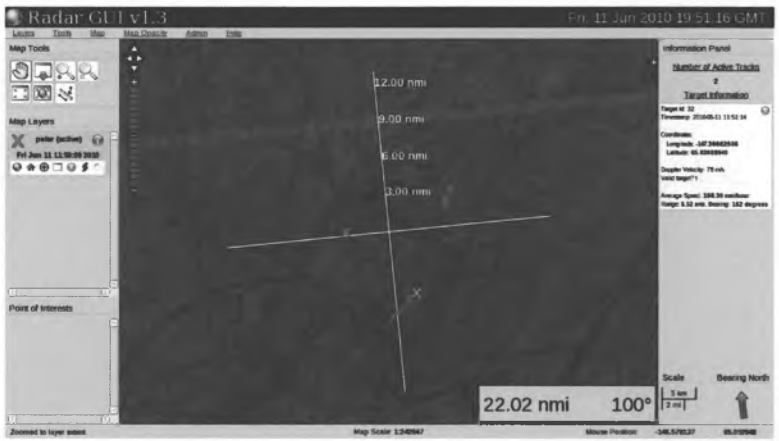
iPASS

UAF's Portable Airspace Surveillance System

Designed and built by UAF for Alaska's airspace monitoring needs

Status

Operational, used in Canada and NASA Certified



Airspace activity monitoring

Monitors airspace use patterns and validates traffic pattern assumptions

Enhanced situational awareness during aircraft or spacecraft operations

Provides real-time position and track of local airspace activity to assist in traffic avoidance

Alaska Center For UAS Integration RDT&E

- Created by Board of Regents Dec 2012
- Three integrated focus areas
  - Engineering - develop technical capabilities to meet new requirements
  - Application Development - drive system capabilities to expand uses and users
  - Training & Education - develop humans to develop, maintain & operate systems
- Within GI & UAF, but named as overall for UA
- Situated to exploit FAA opportunities - Arctic airspace, FAA Test Site

UNIVERSITY of ALASKA
Many Traditions One Alaska

POKER FLAT RESEARCH RANGE
FAIRBANKS, ALASKA

Volume Number: **VII**

Document File Name: **AKUNV-0701.docx**

Solicitation Number: **DTFACT-13-R-00002**

Applicant's Name: **University of Alaska**

Table of Contents

9.2.7. Economic Impact Assessment (SIR 9.2.7) 2
UAS Activity in Alaska, Hawaii, and Oregon 2
Recent UAS Funding in Alaska, Hawaii, and Oregon 3
Leveraging Current Research Institutes, Community Colleges, and Training Centers 4
Expansion of Existing Businesses and Attracting New Business Investment 4
Infrastructure 5
Quantifying the PPUTRC's Economic Impacts 6
Employment Resulting from UAS and Test Site Operations 6
Labor Income Resulting from UAS and Test Site Operations 7
Output, Value Added, & State Income Taxes Resulting from UAS and Test Site Operations 8

List of Acronyms

ACUASI	Alaska Center for Unmanned Aircraft Systems Integration
AUVSI	Association for Unmanned Vehicle Systems International
BMCC	Blue Mountain Community College
COA	Certificate of Authorization
COCC	Central Oregon Community College
ERAST	Environmental Research Aircraft and Sensor Technology
FAA	Federal Aviation Administration
FY	Fiscal Year
IMPLAN	Impact Analysis for Planning by MIG, Inc.
iPASS	Internet-Portable Aerial Surveillance System
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
OSU	Oregon State University
OTA	Other Transactional Agreement
PFRR	Poker Flat Research Range
PPUTRC	Pan-Pacific UAS Test Range Complex
SIR	Screening Information Request
UAF	University of Alaska Fairbanks
UAF CEM	University of Alaska Fairbanks College of Engineering and Mines
UAF CTC	University of Fairbanks Community and Technical College
UAF-GI	University of Alaska Fairbanks Geophysical Institute
UAS	Unmanned Aircraft System

9.2.7. Economic Impact Assessment (SIR 9.2.7)

The Pan-Pacific Unmanned Aircraft Systems Test Range Complex (PPUTRC) is proposed as a Federal Aviation Administration (FAA) test site with 13 test ranges in Alaska, Hawaii, and Oregon. Successful PPUTRC designation would promote new construction, improve existing infrastructure, leverage current research institutions, and attract business investments for complementary assets throughout the service and supply chain in all three states. The economic impact of this activity would be substantial. The PPUTRC is projected by 2017 to increase employment in Alaska, Hawaii, and Oregon by approximately 1,429 jobs, labor income by $76 million, output by $334 million, total value added by $134 million, and government revenue via income taxes by $6 million. This new economic activity would represent significant benefits to the local economies surrounding the test ranges as well as throughout each state's economy.

UAS Activity in Alaska, Hawaii, and Oregon

Existing UAS activity in Alaska, Hawaii, and Oregon benefit from government facilities (e.g. numerous military bases, universities, and maritime assets), geographic diversity (e.g. tropical to arctic climates, oceanic or mountainous landscapes, and up/down weather fronts), and wide open airspace in largely unpopulated areas.

The ACUASI at the University of Alaska Fairbanks (UAF) leads the PPUTRC. The formal PPUTRC team includes over 80 businesses, universities, tribes, and economic development organizations in Alaska. UAF has actively managed UAS operations since 2004. The ACUASI was formed in 2012 to enhance UAS research in Alaska. ACUASI and the UAF Geophysical Institute have developed and flown a variety of *in-situ* and remote sensing instruments on various UAS in Alaska and throughout the world. Scientific and research UAS campaigns undertaken in Alaska over the past decade include supporting observation and monitoring sea lions in the Aleutian Islands, weather forecasting, volcanic plume monitoring, atmospheric sampling during wildfires, monitoring of sea ice build ups, and oil spill mapping. Commercial applications trialed in Alaska include whale monitoring, cadastral mapping, maritime navigation support, industrial plant monitoring, and environmental clean-up. This experience, coupled with UAS Test Site status, would leverage a variety of new economic activities in Alaska.

Hawaii offers many unique qualities that make UAS operations appealing. These include: (1) expansive over-water areas unencumbered by other aviation uses, (2) proximity to U.S. Pacific Command - a significant user of future UAS systems, (3) opportunities for joint operations with the Pacific Missile Range Facility - a major test range on Kauai, and (4) opportunities for long-range point-to-point tests with partner ranges in Alaska and Oregon. The Hawaii ranges have proven an important focus for the development of scientific applications of UAS, with significant milestones including test flights of the Aerovironment Pathfinder, Pathfinder Plus, and Helios solar-hybrid propulsion high altitude long endurance UAS between 1997 and 2001. Scientific applications led by U.S. Federal agencies have recently seen Hawaii emerge as a focal point for NOAA's exploration of UAS as a tool for marine park surveillance. NOAA has used UAS to monitor Papahanaumokuakea Marine National Monument since 2007 and performed initial trials using small hand launched systems in mid-2012.

The Oregon-based PPUTRC team members include 16 businesses, universities, tribes, and economic development organizations. Additionally, six committed team partners will convert to

formal team members upon FAA Test Site designation award to PPUTRC. Engagements are also planned with a wide ranging network in Oregon – including the 111 AUVSI members and numerous startup companies, primarily in sensor, robotics, and other supporting technologies. Oregon has historically been more engaged in design, development, and manufacture of UAS systems and subsystems. The two largest Oregon UAS firms are Insitu (manufacturing) and FLIR Systems (sensors). The main Oregon firm involved in UAS applications has been Near Space Corporation. NSC uses very high altitude unmanned balloons and gliders to perform scientific and commercial test activities, ranging from data gathering on behalf of government agencies to near-space testing of hardware and sensors for commercial firms. NSC is opening a new $6 million flight test and operations facility at the Tillamook airport on the Oregon coast. Existing UAS activity also includes the Oregon Army National Guard operations in Pendleton. Oregon's UAS efforts are synergistic with a separately funded ground vehicle innovation initiative, Drive Oregon, which requires systems that can be spun out of UAS: quiet, efficient motors, lightweight composite designs, and navigation systems. The potential economic benefits of the Test Sites as well as NAS integration are particularly strong for Oregon's already significant aircraft manufacturing sector.

Recent UAS Funding in Alaska, Hawaii, and Oregon

Since 2004, 9 Alaska contractors have received direct U.S. federal agency contracting for UAS goods and services. The largest federal contract in Alaska is a 5-year standing services award worth $47 million from the U.S. Navy to the University of Alaska in 2010 for UAS payload integration and flight test services. The second major award made since 2004 to an Alaska firm consists of a series of pacts totaling $17 million from the U.S. State Department to Anchorage-headquartered Kuk Construction (subsidiary of Olgoonik Development, an Alaskan Native Corporation) for the provision of UAS-based security surveillance services in Iraq in partnership with KBR, Inc. UAF has collaborated with commercial entities such as Idaho Power Company and manufacturers including AeroVironment to conduct surveys and observe environmental impacts. Additionally, UAF is collaborating with BP for oil spill response and flare stack monitoring as well as projects focused on detecting and locating gas and oil pipeline leaks and developing new sensors and processes to identify leaks. Each such project has led to more work as the clients discover the potential of UAS benefits to their businesses.

Hawaii's large military presence has resulted in defense spending as the primary source of federal funding to UAS vendors in the state. Direct defense contracts accounted for 94% of all awards in terms of obligated amounts from 2004-2012, with this rising to 97% when including awards placed by the GSA on behalf of the U.S. Air Force. The remaining awards were placed with Honolulu-based Referentia Systems by NOAA as part of the Papahanaumokuakea Marine National Monument monitoring project. Hawaii supports a dedicated UAS development and manufacturing company, Williams Aerospace, with this small firm currently developing new platforms in the fixed-wing, hand launched micro and medium altitude endurance classes. It is also working to create two commercial UAS services arms, addressing the defense, homeland security, and precision agriculture markets.

In Oregon, a consortium of industry, academia, and public entities has created a 7-year strategic plan to double the size of the UAS industry in the state, with the help of a $2.5 million State of Oregon grant scheduled for the 2013-14 biennium and additional investments of at least $1.15

million from other sources for a total of $3.65 million. The plan specifically creates UAS solutions for commercial applications, and safely integrating those UAS solutions into the NAS. Projects include emergency response; weather; firefighting; search and rescue; wildlife and habitat management; law enforcement; physical and resource surveys (land and water); management of agriculture, livestock, and public lands; and management of public and private infrastructure. Oregon State University (OSU) has already begun UAS flights based on these research objectives.

Leveraging Current Research Institutes, Community Colleges, and Training Centers
ACUASI is collaborating with the College of Engineering and Mines (CEM) and the Community and Technical College (CTC) to integrate UAS engineering, science, and technology into UAF's teaching, research, and service activities. Additionally, ACUASI is working with the CEM to fill a full-time tenure track engineering faculty position with a professor focused on UAS engineering, science, and technology. ACUASI and CTC are working to include UAS technology courses in CTC's aviation curricula to train UAS developers, technicians, and pilots as well as to improve outreach to remote Alaskan villages that could benefit from UAS technologies. Cooperation with the CTC at UAA will add participation of air traffic controllers, offer training for UAS operators, and ultimately build a maintenance program similar to the current FAA certificated Aircraft and Powerplant program.

The University of Hawaii is testing UAS in several of its research programs, evaluating the utility and impact of UAS through analysis of coastal resource management, terrestrial and aquatic environmental monitoring, natural source management and inventory, and human impact studies. University of Hawaii is also developing programs to train students and research professionals on UAS, and plans to integrate this capacity into accredited degree programs.

The new OSU industry-university UAS consortium will depend on test site facilities for collaborative research and development in all phases of operations and applications. Through the Colleges of Engineering, Science, Agriculture, Forestry and Earth, Ocean and Atmospheric Sciences, OSU has expertise and supports ongoing research on control theory and robotics, flexible airframes and flight, sensors, and signal processing, and numerous applications in natural and environmental sciences and environmental monitoring, measuring and management. OSU-Cascades, located in Central Oregon near the Warm Springs and Juniper test ranges, has programs in energy engineering, computer science, natural resources, and business, and plans to add programs designed in conjunction with the UAS industry. OSU-Cascades can also provide on-site facilities for OSU-Corvallis researchers leading projects in the region. Central Oregon Community College (COCC) has one of the largest aviation flight training programs on the West Coast - both fixed wing and rotary. COCC is offering certifications for UAS flight training and plans to develop a program for data analysis of sensors, building on the school's strong geographic information systems program. Additionally, Blue Mountain Community College (BMCC) in Pendleton, Oregon is developing a UAS curriculum for instructional delivery and course certification.

Expansion of Existing Businesses and Attracting New Business Investment
The University of Alaska has spun off at least two companies who intend to test their products on the Pan-Pacific test range. These companies were created by University graduate students

who were expanding their research in sensors for testing in UAS. UA recently received $5 million from the State of Alaska to support the development of a sustainable high-tech industry in Alaska. Already two companies have established satellite offices in Alaska, one of which is creating a new company for UAS aviation technology advancement.

Placement of a UAS Test Site in Hawaii will promote growth within Hawaii and reduce development cycles for manufacturers and researchers. Additionally, it would reduce or eliminate costs to ship sensors, and knowledgeable staff, to mainland test sites to operate and demonstrate systems. Close proximity to a test site in Hawaii will greatly benefit firms such as BAE Systems, Williams Aerospace, and others – including many military and government contractors working with Honolulu Fire Department, Honolulu Police Department, U.S. Civil Air Patrol, U.S. Coast Guard, U.S. Department of Defense, U.S. Department of Homeland Security, U.S. National Guard, and others.

In Oregon more than a dozen companies have said that they will begin testing their sensor packages, propulsion systems, and airframes in Oregon if the Pan-Pacific UAS Test Area is designated as a national Test Site. Additionally, two companies have informally pledged to open satellite offices at a state test range. The PPUTRC will benefit UAS businesses in the Columbia River Gorge. Over the past seven years, the Gorge's UAS industry grew from a small core of 30 people to an employment base of more than 1,400 employees. Many of these new jobs were created by the UAS companies' suppliers. The two largest Oregon UAS manufacturers are Insitu, manufacturer of UAS platforms and subsystems, and FLIR Surveillance Systems, a manufacturer of electro-optic and infrared imaging systems. Insitu is a major global supplier of high endurance, runway-independent UAS. FLIR Surveillance provides more ER and IR imaging systems for unmanned aircraft, unmanned ground, and unmanned maritime platforms than any other company. Activity in the Gorge from firms such as Insitu, FLIR Surveillance Systems, Cloud Cap Technology, and UTC Aerospace has spun off more than 20 local companies. Central Oregon's general aviation aircraft manufacturing industry had a similar growth pattern over a 15-year period, expanding from a core company of about 30 employees (Lancair) to a cluster of 25 companies that now employs nearly 1,200 people. It is anticipated the PPUTRC will help expand these existing businesses in the Gorge and Central Oregon.

Infrastructure

Alaska expects to invest $1.5 million to construct a test site center at its Poker Flat Research Range, as well as develop and acquire mobile test infrastructure such as fixtures, data collection devices and monitoring systems similar to its internet-Portable Aerial Surveillance System (iPASS), a web-based application that merges track information from radar, GPS, and a transponder interrogator/receiver. Additionally, large data collection requirements are expected to drive development of a data center for processing and storage. Venture capitalists have approached the team already, anticipating the value of investing in test site development.

Hawaii's test ranges link to military/restricted areas used for current UAS operations. These sites include the Pohakuloa training area on the Island of Hawaii, Bradshaw and Wheeler Army Airfields on Oahu, and the Pacific Missile Range Facility on Kauai. Other areas under consideration include Upolu and Dillingham Airfields (on the Big Island and Oahu, respectively). Test points within the range would be utilized to support both shore- and ship-

based development, testing and certification of new UAS, training and crew certification of operational UAS, and development of expanded and joint capabilities involving existing communications systems and operations tactics using UAS.

The budget for the $2.5 million Oregon innovation grant envisions spending at least $1.2 million at test ranges for new equipment and/or infrastructure, with the grant providing $300,000, private enterprise providing $750,000, and public entities providing $150,000. Possible infrastructure development proposed with this funding include: portable ground radar units; an automatic dependent surveillance-broadcast ground station or a similar 'sense and avoid' technology system; one or more operations management buildings housing computers, calibration components, baseline sensors with a range of capabilities, data analysis equipment, supporting software, maintenance facilities and machine shops; and ground control stations, an observation tower, and ITAR facilities as needed. Additionally, as noted earlier, Near Space Corporation is preparing to open a new $6 million flight test and operations facility at the Tillamook airport.

Quantifying the PPUTRC's Economic Impacts

The following economic impact projections were developed by McDowell Group, Inc. utilizing flight activity, flight cost, and flight-related staffing data provided by PPUTRC team members. Direct economic activity was measured by approximating preflight administrative costs, site fees per day, operating costs per day, and total flight days from historical data provided by the applicant. Sector-level information was obtained from the applicant concerning number of UAS-related firms and jobs per firm. Direct employment estimates were then coupled with multipliers obtained from the IMPLAN economic impact model to estimate total direct, indirect and induced economic effects. Annual projections from 2014 to 2017 were calculated for each of the 13 ranges utilizing growth rates based on funding forecasts from the Teal Group UAS market profile and forecast report, historical flight activity, and projected growth in flight activity, research, and UAS-related manufacturing as provided by the applicant.

Table 7-1 Summary Impacts of PPUTRC Test Site Designation, 2012-2017

Impact of Test Site Designation				
	2014	2015	2016	2017
Total Employment	**1,065**	**1,260**	**1,335**	**1,429**
Direct Employment	490	571	602	642
Indirect Employment	198	243	259	279
Induced Employment	377	447	474	508
Total Labor Income ($ million)	**$56.9**	**$66.9**	**$70.8**	**$75.6**
Direct Labor Income ($ million)	$26.4	$30.5	$32.2	$34.2
Indirect Labor Income ($ million)	$10.4	$12.5	$13.3	$14.4
Induced Labor Income ($ million)	$20.1	$23.8	$25.3	$27.1
Output ($ million)	**$265.0**	**$301.8**	**$315.9**	**$333.5**
Total Value Added ($ million)	**$109.3**	**$121.9**	**$127.1**	**$133.5**
State Income Taxes ($ million)	**$4.3**	**$5.0**	**$5.3**	**$5.6**

Employment Resulting from UAS and Test Site Operations

In 2014, UAS activity in Alaska, Hawaii, and Oregon is expected to account for 581 direct jobs and a total of 1,254 jobs - including direct, indirect, and induced jobs – from PPUTRC

designation. Approximately 85 percent of that total employment (1,065 jobs) is attributable to Test Site designation. The remaining 15 percent (189 jobs) is expected to occur in the absence of PPUTRC Test Site designation. By 2017, employment will rise to an estimated 904 direct jobs and 1,991 total jobs - with 72 percent of that total employment (1,429) attributable to Test Site designation. A significant number of these direct jobs are expected in smaller communities that tend to have higher unemployment – thus Test Site designation for the PPUTRC will help improve opportunities where they will provide the most benefits.

Table 7-2 Direct Employment, 2012-2017

	Direct Employment					
	2012	2013	2014	2015	2016	2017
Total Direct Employment						
PPUTRC	74	82	581	712	801	904
Alaska Ranges	43	47	129	142	157	173
Hawaii Ranges	-	-	-	72	95	126
Oregon Ranges	31	35	452	498	549	605
Impact of Test Site Designation						
PPUTRC	-	-	490	571	602	642
Alaska Ranges	-	-	77	82	86	91
Hawaii Ranges	-	-	-	72	95	126
Oregon Ranges	-	-	414	417	421	424

Oregon's relatively high direct employment numbers are due to the existing, well-developed aircraft manufacturing sector in Oregon. Oregon is well placed to supply the growing demand for UAS aircraft that will be triggered by UAS integration. Most of the new jobs created in Oregon due to PPUTRC designation include manufacturing jobs (many of which may be created due to designation of test sites anywhere in the U.S.),

Table 7-3 Indirect and Induced Employment, 2012-2017

	Indirect Employment						Induced Employment					
	2012	2013	2014	2015	2016	2017	2012	2013	2014	2015	2016	2017
Total Indirect or Induced Emp.												
PPUTRC	21	24	224	290	328	374	59	65	448	558	629	712
Alaska Ranges	7	8	22	24	27	30	35	39	106	117	129	142
Hawaii Ranges	-	-	-	42	56	74	-	-	-	64	84	111
Oregon Ranges	14	16	202	223	246	271	24	26	342	377	416	459
Impact of Test Site Designation												
PPUTRC	-	-	198	243	259	279	-	-	377	447	474	508
Alaska Ranges	-	-	-	42	56	74	-	-	63	67	71	75
Hawaii Ranges	-	-	185	187	188	190	-	-	-	64	84	111
Oregon Ranges	-	-	13	14	15	16	-	-	313	316	319	321

Labor Income Resulting from UAS and Test Site Operations

In 2014, UAS activity in Alaska, Hawaii, and Oregon is expected to account for $31 million in direct labor income and $67 million in total labor income - including direct, indirect, and induced - from PPUTRC designation. Approximately 84 percent of that total labor income ($57 million)

is attributable to Test Site designation. The remaining 16 percent ($10 million) is that which is expected to occur even if the proposed PPUTRC does not become a Test Site. By 2017, labor income is expected to include $106 million in total direct, indirect and induced labor income - with 71 percent of that total labor income ($76 million) attributable to Test Site designation.

Table 7-4 Direct Income, 2012-2017 ($ million)

	Direct Income					
	2012	2013	2014	2015	2016	2017
Total Direct Income						
PPUTRC	$4.0	$4.4	$31.3	$38.2	$42.9	$48.3
Alaska Ranges	$2.3	$2.6	$7.0	$7.7	$8.5	$9.4
Hawaii Ranges	-	-	-	$3.7	$4.9	$6.4
Oregon Ranges	$1.7	$1.9	$24.2	$26.7	$29.5	$32.5
Impact of Test Site Designation						
PPUTRC	-	-	$26.4	$30.5	$32.2	$34.2
Alaska Ranges	-	-	$4.2	$4.4	$4.7	$5.0
Hawaii Ranges	-	-	-	$3.7	$4.9	$6.4
Oregon Ranges	-	-	$22.2	$22.4	$22.6	$22.8

Table 7-5 Indirect and Induced Labor Income, 2012-2017 ($ million)

	Indirect Labor Income						Induced Labor Income					
	2012	2013	2014	2015	2016	2017	2012	2013	2014	2015	2016	2017
Total Indirect or Induced Emp.												
PPUTRC	$1.1	$1.3	$11.7	$15.0	$17.0	$19.3	$3.5	$3.8	$24.4	$30.1	$34.0	$38.4
Alaska Ranges	$0.4	$0.4	$1.2	$1.3	$1.5	$1.6	$2.2	$2.5	$6.7	$7.4	$8.2	$9.0
Hawaii Ranges	-	-	-	$2.1	$2.7	$3.6	-	-	-	$3.3	$4.3	$5.7
Oregon Ranges	$0.7	$0.8	$10.5	$11.6	$12.8	$14.1	$1.2	$1.4	$17.6	$19.4	$21.4	$23.6
Impact of Test Site Designation												
PPUTRC	-	-	$10.4	$12.5	$13.3	$14.4	-	-	$20.1	$23.8	$25.3	$27.1
Alaska Ranges	-	-	$0.7	$0.8	$0.8	$0.9	-	-	$4.0	$4.3	$4.5	$4.8
Hawaii Ranges	-	-	-	$2.1	$2.7	$3.6	-	-	-	$3.3	$4.3	$5.7
Oregon Ranges	-	-	$9.6	$9.7	$9.8	$9.9	-	-	$16.1	$16.3	$16.4	$16.6

Output, Value Added, & State Income Taxes Resulting from UAS and Test Site Operations

'Output' represents the value of industry production, and 'total value added' is the difference between an industry's total output and the cost of their intermediate inputs. Economic modeling conducted for purposes of this study indicates output in the PPUTRC states attributable to test site designation would climb from $265 million in 2014 to $333 million in 2017. Value added would climb from $109 million to $134 million over the same period.

Designation of the PPUTRC will provide a four-year total of $20 million of income tax revenue to Hawaii and Oregon. The effective income tax rate for these calculations was approximated as 7.5 percent for Hawaii, and 9 percent for Oregon (Alaska has no income tax).

References

Alaska Center for Unmanned Aircraft Systems Integration – Research, Development, Test, and Evaluation. 2012. Proposal for the Creation of the Alaska Center for Unmanned Aircraft

Systems Integration – Research, Development, Test, and Evaluation (ACUASI – RDT&E). http://www.alaska.edu/files/bor/121206Ref01_Alaska_Center_Unmanned_Aircraft_Systems_ACUASI_RDTE.pdf.

Association for Unmanned Vehicle Systems International. 2013. The Economic Impact of Unmanned Aircraft Systems Integration in the United States.

Economic Development of Central Oregon. 2011. Central Oregon Unmanned Aircraft Systems.

MIG. 2012. IMPLAN Version 3.0.

Pan-Pacific Unmanned Aircraft System Test Range Complex. 2013. Volume III: Research Goals and Objectives Application.

Teal Group Corporation. 2008. World Unmanned Aerial Vehicle Systems: Market Profile and Forecast.

United States of America Federal Aviation Administration. 2013. Fact Sheet. http://www.faa.gov/news/fact_sheets.

United States of America Federal Aviation Administration. 2008. Interim Operational Approval Guidance 08-01 Aviation Safety: Unmanned Aircraft Program Office, AIR-160. http://rmgsc.cr.usgs.gov/uas/pdf/uas_guidance08-01.pdf.

United States of America Government Accountability Office. 2013. Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development.

United States of America Spending Government Site. 2013. http://usaspending.gov/explore.

Unmanned Aircraft Systems Project Proposal to the Oregon Innovation Council (OR InC). 2012.

what would you attempt to do if you knew you could not fail?

(unknown)

NOTICE U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

N 8900.207

National Policy

Effective Date:
1/22/13

Cancellation Date:
1/22/14

SUBJ: Unmanned Aircraft Systems (UAS) Operational Approval

1. Purpose of this Notice. This notice provides policies necessary for reviewing and evaluating the safety and interoperability of proposed Unmanned Aircraft Systems (UAS) flight operations conducted within the United States (U.S.) National Airspace System (NAS) for the Aviation Safety (AVS) Flight Standards Service (AFS), UAS Integration Office (AFS-80), when assessing applications for a Certificate of Waiver or Authorization (COA) or special airworthiness certificate.

2. Audience. This notice applies to AFS divisions at the Federal Aviation Administration (FAA) Washington headquarters (HQ) and regional field offices.

3. Where You Can Find This Notice. You can find this notice on the MyFAA Web site at https://employees.faa.gov/tools_resources/orders_notices/. Inspectors can access this notice through the Flight Standards Information Management System (FSIMS) at http://fsims.avs.faa.gov. Air carriers and operators can find this notice on the FAA's Web site at: http://fsims.faa.gov. This notice is available to proponents and the public at http://www.faa.gov/regulations_policies/orders_notices.

4. Background.

a. UAS Operations. UAS operations have increased dramatically in both the public and private sectors. This proliferation has introduced greater exposure and elevated risk to the safety of operations within the NAS. This growth in UAS operations has increased the number of applications for operational approvals and increased demand on the FAA to process them. For these activities, the development of a notice is required for the FAA to use when evaluating applications for COAs and special airworthiness certificates.

b. Policy. Policy identifies Unmanned Aircraft (UA) as "aircraft" flown by a "pilot" regardless of where the pilot is located. Aircraft and pilots must demonstrate compliance with applicable sections of Title 14 of the Code of Federal Regulations (14 CFR) to operate in the NAS. However, UA are not compliant with certain sections of 14 CFR. For instance, the absence of an onboard pilot means that the "see-and-avoid" provisions of 14 CFR part 91, § 91.113, cannot be satisfied. Without an onboard pilot, there is a significant reliance on the command and control link, and a greater emphasis on the loss of functionality associated with lost link. Furthermore, for air traffic control (ATC) operations requiring visual means of maintaining

in-flight separation, the lack of an onboard pilot does not permit ATC to issue all of the standard clearances or instructions available under the current edition of FAA Order 7110.65, Air Traffic Control. Consequently, to ensure an equivalent level of safety, UAS flight operations require an alternative method of compliance (AMOC) or risk control to address their "see-and-avoid" impediments to safety of flight, and any problems they may generate for ATC. In the future, permanent and consistent methods of compliance will be needed for UAS operations in the NAS without the need for waivers or exemptions.

5. Consensus Opinion. This notice is subject to continuous review, will be updated when appropriate, is not meant as a substitute for any regulatory process, and was jointly developed by and reflects the consensus opinion of:

- Flight Technologies and Procedures Division (AFS-400);
- UAS Integration Office (AFS-80) and the ATO component of AFS-80; and
- Aircraft Certification Service, Production & Airworthiness Branch (AIR-240).

Note: In general, and as a minimum, proponents must observe all applicable regulations of 14 CFR parts 61 and 91. This notice identifies acceptable AMOC with the regulations when evaluating requests for approval of proposed UAS operations. Refer to the following Web site for a listing of regulations: http://www.faa.gov/regulations_policies/faa_regulations/.

6. Discussion. This notice represents the culmination of input from government agencies, industry, and user stakeholders along with best practices and procedures that have been used by FAA in prior approvals for UAS applications for COAs or special airworthiness certificates. The material presented in this notice represents the process and procedures necessary for approving applications for UAS flight operations. However, because of the uniqueness of various UAS flight operations, each application must be evaluated on its own technical merits, including operational risk management (RM) planning. Each application may require unique authorizations or limitations directly related to the specific needs or capabilities of the UAS and/or the proposed specific mission and operating location.

7. Applicability and Approval Process Criteria. The applicability and process to be used in UAS operational approval are dependent on whether the proposed UAS operation within the territorial airspace of the United States (the airspace above the contiguous United States, Alaska, Hawaii, U.S. territories, and U.S. territorial waters) is defined as public or civil (see 14 CFR part 1, § 1.1 and Public Law 110-181, "The National Defense Authorization Act of 2008"). UAS operations outside the territorial airspace of the U.S. will be classified as either state or civil operations in accordance with international law. A public operation is one that is intrinsically governmental in nature (i.e., Federal, State, and local agencies). Proponents requesting approval of public aircraft operations by UAS will use the COA application process. In contrast, proponents for civil operations approval will use the special airworthiness certificate process. Part 91, § 91.319(a)(2) specifically prohibits operation of an aircraft that has an experimental certificate from "carrying persons or property for compensation or hire."

a. Coordination and Approval. Regardless of the process for the authorization approval, COA applications for UAS flight operation approvals will be coordinated through the ATO component of AFS-80 and AVS. Special airworthiness certificates will be coordinated through the Aircraft Certification (AIR-240) staff as well as the ATO and AFS component of AFS-80 for final approval and disposition.

b. Applicability and Methods of Authorization. Operational policy in this notice applies to both public and civil operations and certain state aircraft operations.

(1) Applicability. These procedures are applicable for all operations in the contiguous United States, Alaska, Hawaii, U.S. territories, and international airspace in the Flight Information Regions (FIR) delegated to the United States where the FAA is the Air Traffic Service (ATS) provider. These procedures do not apply to the territorial airspace of another sovereign country that lies within FIRs delegated to the United States where the FAA is the ATS provider, except by agreement with that country, or airspace in FIRs delegated to other countries. All UAS proponents, operators, and pilots must observe all applicable regulations of 14 CFR.

(a) In general, specific authorization to conduct UAS operations in the NAS outside of active Restricted and Warning Areas designated for aviation use, or approved Prohibited Areas, must be requested by the proponent. Airspace inside buildings or structures is not considered to be part of the NAS and is not regulated. (Refer to the current edition of Order JO 7400.8, Air Traffic Organization Policy.)

(b) This notice and the processes prescribed do not apply to hobbyists and amateur model aircraft users when operating unmanned systems for sport and recreation. Those individuals should seek policy under the current edition of Advisory Circular (AC) 91-57, Model Aircraft Operating Standards. AC 91-57 is not to be used as a basis of approval for operation of any other aircraft, including by Federal, State, and local governments, commercial entities, or law enforcement.

(c) This notice and the processes prescribed also do not apply to UAS operations in FAA-controlled international airspace by an agency of, or a contractor to, the Federal government when those operations are appropriately designated as State aircraft operations and are operated under "due regard" rules and procedures established by the Federal agency responsible for the operation. The designation of flight operations as State aircraft operations normally are made in coordination with the U.S. Department of State. This notice and the processes prescribed do, however, apply where the responsible Federal agency either has not established a formal set of rules and procedures for "due regard" operations, or is not operating the UAS under "due regard" rules and procedures in FAA-controlled international airspace. This notice and the processes prescribed also apply to all UAS operations by an agency of, or a contractor to, the Federal government that transit through U.S. territorial airspace en route to or from international airspace. See Appendix F, UAS COA Requirement. The "due regard" option is not available for state aircraft operations transiting through U.S. territorial airspace en route to or from international airspace.

(d) Oceanic Operations Within Warning Areas. UAS operations contained within Warning Areas are handled in the same manner as those operations conducted in active Restricted and approved Prohibited areas; that is, neither specific FAA approval nor observers or chase aircraft are required by the FAA.

(e) The only public aircraft that can fly under "due regard" are U.S. government aircraft designated as State aircraft.

(2) Methods. The two methods of approval are the issuance of either a COA for public aircraft operations or a special airworthiness certificate for civil operations. In the case of public aircraft operations, the operating entity applying to conduct the UAS operation must comply with its own processes, policies, and standards in the following areas, in addition to complying with all applicable safety provisions in all other parts of 14 CFR:

- Pilot certification,
- Crew certification,
- Recent pilot experience (or, currency),
- Medical certificates, and
- Airworthiness of public UAS.

Note: If no established public entity processes, policies, or standards exist, it is highly recommended that the public agency/department apply the specifics outlined in this notice and comply with the provisions of 14 CFR applicable to civil UAS operations.

8. COA for Public Operations.

a. Applications. Applications for a COA are only accepted from entities that intend to conduct public aircraft operations. An application may be referred to the FAA Office of the Chief Counsel (AGC-200) for determination of the status of a proponent as a government entity under the public aircraft statute. The duration of COAs complies with the time limitations specified under the current edition of FAA Order 7210.3, Facility Operation and Administration. COAs may be issued for a lesser duration if requested or deemed appropriate. COAs are not required for operations conducted within active Restricted or Warning Area airspace designated for aviation use, or approved Prohibited Areas with permission from the appropriate authority or using agency of that airspace. (Refer to the current edition of Order JO 7400.8, Special Use Airspace.)

b. Approving and Reviewing Authority. AFS-80 is responsible for determining whether the proponents' proposed UAS operations can be conducted safely and responsibly in the NAS, and that they comply with all COA limitations and provisions.

(1) In accordance with FAA Order 7210.3, "As a general rule, a waiver or authorization should be canceled when it is no longer required or there is an abuse of its provisions or unforeseen safety factors develop. Failure to comply with the waiver or authorization is cause for cancellation."

(2) The FAA has the authority to suspend or cancel the COA, or to delay any activities if there is a violation of the terms in the COA, or if the safety of persons or property on the ground or in the air is determined to be in jeopardy. That may include, but is not limited to:

- Incidents or accidents occurring during UAS operations in the NAS;
- Habitual noncompliance with administrative requirements, such as failure to provide the FAA with monthly reports on the number of flights, pilot duty time, or unusual equipment malfunctions (e.g., a malfunction or failure of ground control station (GCS) flight control hardware or software (other than loss of control link); a power plant failure or malfunction; a deviation from any provision contained in the COA);
- Deviations from ATC instructions, operational, or coordination issues; and
- Events of intermittent or persistent lost-link as described in the COA or events determined to pose as a risk to the safety of the NAS.

(3) COA suspensions and cancellations are not automatic. Whenever possible, a documented conversation, between the FAA and the proponent, will happen before the suspension/cancellation is issued. Timely and transparent responses to accidents, deviations, and similar safety-related events are expected.

c. Accident and Incident Notification and Investigation. The current edition of FAA Order 8020.11C, Aircraft Accident and Incident Notification, Investigation, and Reporting, and Title 49 of the Code of Federal Regulations (49 CFR) part 830, outlines reporting procedures for accidents and incidents involving civil aircraft and certain public aircraft. All accidents and incidents involving fatalities, injuries, property damage, and fly-away by civil aircraft and those public aircraft subject to part 830 require FAA notification within 24 hours. No additional flights by those aircraft under this COA are allowed before notification. An immediate investigation is required, and when requested to do so, UAS proponents are expected to provide copies of written aircraft accident/incident reports to AFS-80 for review. In accordance with 49 CFR part 1520, § 1520.5, reports will not be released outside of government channels without originator permission.

d. General COA Process. The ATO component of AFS-80 is responsible for the COA process. Applications can be made two ways:

(1) On the Internet using the UAS COA Online System at https://ioeaaa.faa.gov. The UAS COA Online System requires a user name and password; a support desk phone number and e-mail address is provided to assist with obtaining an account.

(2) Using FAA Form 7711-2, Application for Certificate of Waiver or Authorization, available online at http://www.faa.gov/documentLibrary/media/form/faa7711-2.pdf. The completed form can be mailed to: FAA Headquarters, Unmanned Aircraft Systems Integration Office, 490 L'Enfant Plaza SW, Suite 3200, Washington, DC 20024. Mail submittal may encounter significant delay due to current U.S. Postal Service security screening procedures in place.

e. Operational Review. Prior to issuance of a COA, air traffic specialist components of AFS-80 conduct an operational validation that addresses ATC processes. Next, an aviation safety inspector (ASI) evaluates each application to determine if risks to the NAS associated with the operation have been acceptably mitigated. Both the ASI and ATC requirements are merged into the final COA.

f. Safety Risk Management (SRM) Process. ASIs and other FAA personnel use SRM principles outlined in the current edition of AC 120-92, Safety Management Systems for Aviation Service Providers, to maintain or improve the safety of the NAS by identifying safety risks, hazards, and mitigations associated with proposed UAS operations. When deemed appropriate, Safety Risk Management Documents (SRMD) are created through SRM reviews of specific operations or of risks associated with UAS operations in various classes of airspace. SRM reviews may result in the incorporation of additional mitigations or controls into all or some COAs.

g. National Security Considerations. When appropriate levels of Department of Defense (DOD) or Department of Homeland Security (DHS) declare a UAS operation to be a matter of national security, the FAA may approve an application for a COA which, under normal circumstances, might not otherwise conform to the guidelines set forth in this notice. In this case, national security may override risk mitigation requirements. Such requests to the FAA Administrator will originate from an equivalent level of authority from the proponent's parent organization.

h. Special COA.

(1) National Disaster COA. Due to the unpredictability of national disasters, a National Disaster COA is issued in two parts. In part 1 of the COA, AFS-80 completes an evaluation, excluding the location of the disaster. All known information is inserted into a template and signed by appropriate FAA authority. Once the specific location is identified, this information, along with the specific operation, is inserted into part 2 of the COA in the form of an attachment. Part 2 of the COA must then be signed by appropriate FAA authority, which completes and establishes a valid COA.

(2) Emergency COA. An emergency UAS COA may be considered when all of the following conditions apply:

(a) A situation exists that is defined as a condition of distress or urgency, where there is, or that has, the extreme possibility of loss of life, and

(b) The proponent has determined that manned flight operations cannot be conducted efficiently, and

(c) The proposed UAS is operating under a current approved COA for a different purpose or location.

Note: Requests for UAS COAs that fall outside of these parameters will be processed through the normal online COA application process. Emergency UAS COAs will not be considered for:

- Demonstration flights,
- Flights to test capabilities,
- Training,
- Flights in Class B Airspace, or
- Flights over populated areas, unless a suitable mitigation strategy is proposed and found to be acceptable.

9. Special Airworthiness Certificate for Civil UAS Applicants.

a. Airworthiness Determination. Civil applicants may apply for a special airworthiness certificate from the FAA. The proponent is required to submit the requisite data to support a determination that the aircraft and its systems, including the control station (CS), are designed, built, and maintained in a safe and airworthy condition.

b. Special Airworthiness Certificate Issuance. Special airworthiness certificates are typically issued to proponents wishing to conduct UAS research and development (R&D), crew training, and market surveys under 14 CFR part 21, § 21.191. Special airworthiness certificates are issued in accordance with FAA Order 8130.34, Airworthiness Certification of Unmanned Aircraft Systems and Optionally Piloted Aircraft, current edition. Refer to Order 8130.34 for in-depth information on special airworthiness certificates.

c. Proponents with both a COA and Special Airworthiness Certification. In cases where a proponent has been issued a special airworthiness certificate, and is concurrently eligible to operate a corresponding UAS on a COA as a public aircraft operation, the proponent must elect, prior to each flight, which authority is to be used to conduct the flight. The use of both a special airworthiness certificate and a COA on a single flight is not permitted.

d. General Process for Civil UAS Operations. For civil UAS operations, the Aircraft Certification Service, Production and Airworthiness Division (AIR-200) at FAA HQ, is responsible for the issuance of special airworthiness certificates according to FAA Order 8130.34. The issuance of a special airworthiness certificate is coordinated with AIR-200, AFS-80 and the ATO component of AFS-80, and AVS at the HQ and regional levels. A thorough review is conducted by the FAA to evaluate the system's airworthiness and operational specifications. In addition, the FAA reviews and accepts mitigations developed by the proponent to meet acceptable standards of safety.

10. UAS Airworthiness. All UAS must be in an airworthy condition to conduct flight operations in the NAS. An "airworthy condition for UAS subject to a COA" means that the UAS meets the applicable standards and requirements of its operating agency and is capable of operating in compliance with the applicable requirements in 14 CFR part 91. The FAA recognizes that some of the requirements can differ from those for manned aircraft and appropriate changes can be defined. As with airworthiness standards, maintenance technician requirements will be addressed as part of the review process.

a. Public Aircraft Proponents. The proponent must provide an airworthiness statement specifying compliance with the proponent's applicable airworthiness criteria. Airworthiness statements must be provided on agency letterhead and include:

- The date the statement is effective,
- A signature of the responsible certifying authority within the agency,
- A point of contact (POC), and
- Any warnings/limitations.

(1) Airworthiness statements are generally written for one UAS. If more than one UAS model is included on a single airworthiness statement, each UAS will be listed and specific information for each UAS will be included in the statement. Airworthiness statements with an expiration date must remain current for the duration of the COA including extensions. If a new airworthiness statement is issued during the period the COA is active, a copy of the airworthiness certificate must be provided to AFS-80.

(2) Examples of acceptable policy/criteria include, but are not limited to:

- Department of Defense (DOD) Handbook, MIL-HDBK 516B, Airworthiness Certification Criteria;
- Air Force Policy Directive (AFPD) 62-6, USAF Aircraft Airworthiness Certification;
- Army Regulations (AR) 70-62, Airworthiness Qualification of Aircraft Systems; or
- Naval Air Systems Command Instruction, NAVAIRINST 13034.1 series, Flight Clearance Policy for Air Vehicles and Aircraft Systems.

b. Civil Aircraft Proponents. Approvals for civil applications using the special airworthiness certificate process receive their airworthiness certification from the FAA.

c. Continued Airworthiness.

(1) Public Aircraft. Proponents for UAS used in public aircraft operations should follow their own agency's procedures and guidelines to maintain continued airworthiness at a level which ensures they continue to operate the aircraft safely.

(2) Civil Aircraft. Proponents for civil UAS operational approvals must address continued airworthiness procedures as part of their application. Civil UAS should be maintained and must conform to the same airworthiness standards defined in 14 CFR parts under which UAS are intended to be operated. It is highly recommended that all proponents provide the following information:

- A Continuing Airworthiness Program,
- A maintenance training program,
- Any unique skill sets or maintenance practices relating to their aircraft and/or aircraft operations that may be outside the current scope and practices of manned aviation, and
- A process to report any applicable data relating to the operation and maintenance of the UAS.

d. Database and Recordkeeping. All information received from UAS proponents aids the FAA in establishing a database for the existing UAS types and operations. This data is critical to our development of future certification criteria for both systems and pilots. It expedites the regulatory process for UAS and allows the FAA to have historical data from which to base current and future UAS policy. Accurate recordkeeping is essential in assuring positive operational and quality airworthiness control. In accordance with 49 CFR § 1520.5, reports will not be released outside of government channels without originator permission.

11. Flight Operations of a UAS.

a. Applicability and Requirements. This notice applies to UAS operations conducted in the NAS other than in active Restricted and Warning Areas designated for aviation use or approved Prohibited Areas. The FAA requires aircraft to operate safely among all users of the NAS, including non-cooperative aircraft (e.g., aircraft operated without a transponder), and other airborne operations not reliably identifiable by ATC radar (e.g., balloons, gliders, parachutists). Unless otherwise specifically authorized, UAS operators must use observers, either airborne or ground-based, to comply with 14 CFR part 91 requirements.

b. Risk Mitigation. While considerable work is ongoing to develop a certifiable detect, sense, and avoid system as an AMOC with the see-and-avoid aspect of §§ 91.113 and 91.115, no current solution exists. As a result, compliance with the see-and-avoid requirement and navigational awareness are primary concerns in UAS operational approvals leading to imposition of AMOC. Risk mitigation for these two issues is normally based on the use of observers or other methods of maintaining flight separation and collision avoidance or 'segregation'; however, they may also include other concepts or systems that a proponent may propose for FAA review. The FAA only approves UAS flight operations that can be conducted at an acceptable level of safety. Refer to the current editions of AC 120-92 and FAA Order 8000.369, Safety Management System Guidance.

> **Note:** Risk mitigations that depend on the establishment of new types and categories of airspace are extremely difficult and time-consuming. The NAS is established and configured through a rigorous regulatory process. Risk mitigations that result in the prohibition of the public's right to transit airspace will require a very long lead time with no guarantee that they will be approved.

(1) Proponents proposing see-and-avoid strategies in lieu of visual observers (VOs) are required to support proposed mitigations with system safety cases which indicate the operations can be conducted safely. Acceptable system safety cases must include a hazard analysis, risk assessment, and other appropriate documentation that identifies the level of risk.

(2) It is the proponent's responsibility to demonstrate that the risk of injury to persons or property along the flightpath is appropriately mitigated. Aircraft with performance characteristics that impede, delay, or divert other normal air traffic operations may be restricted in their operations.

12. System Considerations for UAS.

a. Traffic Alert and Collision Avoidance Systems (TCAS). The use of TCAS by UAS has not been validated as an acceptable alternative for see-and-avoid requirements, and is not an approved means of mitigation for UAS see-and-avoid requirements or strategies.

b. Onboard Cameras/Sensors. Although onboard cameras and sensors positioned to observe targets on the ground have demonstrated some capability, their use in detecting airborne operations for the purpose of segregation is still quite limited. To date, these types of systems have not been approved as a sole mitigation in the see-and-avoid risk assessment.

c. Use of Equipment in Lieu of VOs.

(1) Any equipment proposed for use on UAS to accomplish the function of see-and-avoid in lieu of VOs must:

- Be certified as an aircraft system and equipment using standards, requirements, and processes commensurate with installation of equipment in aircraft by a recognized airworthiness authority, and
- Meet the requirements of 14 CFR part 25, § 25.1309, or equivalent process, for any UAS installation, regardless of its size, performance, or maximum takeoff weight.

Note: For other equipment that is not proposed for use in meeting see-and-avoid requirements, § 23.1309, or equivalent process, should be used.

(2) It is the responsibility of the proponent to show that the contemplated standards, requirements, and processes meet an equivalent level of safety.

d. Radar and Other Sensors. If special types of radar systems or other sensors are utilized to mitigate risk, the proponent must provide supporting data which demonstrates the following can be accomplished safely:

- Both cooperative and non-cooperative traffic can be detected and tracked to ensure appropriate separation and collision avoidance,
- The proposed system can effectively mitigate a potential collision,
- Operators are suitably trained and equipped to use them effectively, and
- Procedures are in place for the pilot in command (PIC) to effectively use the data.

e. Lost Link Procedures. There are many acceptable approaches to satisfy lost link requirements. The intent of any lost link procedure is to ensure airborne operations remain predictable. Proponents will comply with the UAS lost link procedures as specified in the COA.

Note: Lost link is not considered fly-away. Refer to definitions in Appendix A.

(1) Unless otherwise authorized, lost link solutions must comply with the last ATC clearance (if ATC clearance is required), for a period of time sufficient for ATC to ensure conflict resolution without loss of required separation.

(2) Lost link procedures are pre-coordinated by AFS-80 with the appropriate ATC facility and included in the COA. They include, at a minimum, lost link route of flight, transponder use, lost link orbit points, communications procedures, and pre-planned flight termination points (FTP) or other contingency planning measures in the event recovery of the UAS is not feasible.

(3) If lost link occurs within a Restricted Area, Warning Area, or Class A airspace, or lost link procedure takes aircraft into one of these areas, the aircraft will not exit that airspace, unless otherwise authorized, until link is re-established. All exceptions will be submitted as part of the COA application to AFS-80 for review.

(4) Unless otherwise authorized, lost link procedures will conform to the Contingency Planning Limitations in Appendix E and in general, include the following:

- Limiting of UAS operations to operations over water or sparsely populated areas over the ground to transit to another Restricted Area, Warning Area, or to a pre-planned lost link orbit point within visual line-of-sight to re-establish link. (The UAS lost link procedure will not transit over fixed structures on the water.)
- Lost link programmed procedures will avoid unexpected turn-around and/or altitude changes and will provide sufficient time to communicate and coordinate with ATC.
- Lost link orbit points will not be contained within any published holding area, airway, Jet route, T route, or other area navigation (RNAV) published route.

(5) If the link is not re-established within a pre-determined time as defined by the FAA-approved COA, the aircraft may:

- Autoland; however, the aircraft will not exit the Restricted Area or Warning Area in accordance with subparagraph 12.e.(3) above,
- Proceed to another lost link point (LLP) in an attempt to regain communication link, or
- Proceed to an FTP or the location specified in other contingency planning measures for flight termination.

Note: LLPs may be used as FTPs. In this case, the aircraft may loiter at the LLP/FTP until link is re-established or fuel exhaustion occurs.

- UAS without auto-land capability will proceed to a pre-planned FTP or other acceptable contingency planning option prior to fuel exhaustion.

(6) Refer to Appendix E for more Contingency Planning Limitations.

f. Flight Termination System (FTS). It is highly desirable that all UAS have system redundancies and independent functionality to ensure the overall safety and predictability of the system. UAS that lack system redundancies may be required to have an independent FTS that can be activated manually by the UAS PIC to safeguard the public.

g. Spectrum Authorization.

(1) Every UAS proponent must have the appropriate National Telecommunications and Information Administration (NTIA) or Federal Communications Commission (FCC) authorization/approval to transmit on the radio frequencies (RF) used for UAS uplink and downlink of control, telemetry, and payload information.

(2) Non-Federal public agencies, such as universities and State/local law enforcement, and all civil UAS proponents generally require a license from the FCC as authorization to transmit on frequencies other than those in the unlicensed bands (900 megahertz (MHz), 2.4 gigahertz (GHz), and 5.8 GHz). This generally will be in the form of an Experimental Radio License or a Special Temporary Authority (STA) issued by the FCC. Non-Federal public agencies and civil UAS proponents that operate systems using frequencies assigned to the Federal government (e.g., the DOD) must demonstrate they have the proper authorization through FCC-issued documentation.

(3) DOD agencies will typically demonstrate UAS spectrum authorization through an STA issued by NTIA or a frequency assignment in the NTIA-administered Government Master File (GMF). Authorizations issued under Title 47 of the Code of Federal Regulations (47 CFR) part 300, in the NTIA Manual, Chapter 7, paragraph 7.11, Use of Frequencies by Certain Experimental Stations, are not appropriate for UAS operations.

(4) Federal public agencies other than DOD, such as National Aeronautics and Space Administration (NASA), U.S. Coast Guard (USCG), and U.S. Customs and Border Protection (USCBP), also need an STA issued by NTIA or a frequency assignment in the NTIA-administered GMF. This is especially important for systems designed to operate on frequencies assigned to DOD.

13. Operational Requirements for UAS. Unless operating in an active Restricted or Warning Area designated for aviation use, or approved Prohibited Areas, UAS operations must adhere to the following requirements.

a. Observer Requirement. Visual flight rules (VFR) UAS operations may be authorized utilizing either ground-based or airborne VOs onboard a dedicated chase aircraft. A VO must be positioned to assist the PIC, to exercise the see-and-avoid responsibilities required by §§ 91.111, 91.113, and 91.115 by scanning the area around the aircraft for potentially conflicting traffic and assisting the PIC with navigational awareness.

(1) VOs:

(a) Must assist the PIC in not allowing the aircraft to operate beyond the visual line-of-sight limit, and

(b) Must be able to see the aircraft and the surrounding airspace sufficiently to assist the PIC with:

- Determining the UA's proximity to all aviation activities and other hazards (e.g., terrain, weather, structures), and

- Exercising effective control of the UA, and
- Complying with §§ 91.111, 91.113, and 91.115, and
- Preventing the UA from creating a collision hazard, and

(c) Must inform the PIC before losing sufficient visual contact with the UA or previously sighted collision hazard. This distance is predicated on the observer's normal vision. Corrective lenses, spectacles, and contact lenses are permitted.

(2) Because of field of view and distortion issues with aids to vision such as binoculars, field glasses, night vision devices, or telephoto lenses, these are allowed only for augmentation of the observer's visual capability; they cannot be used as the primary means of visual contact. When using other aids to vision, VOs must use caution to ensure the aircraft remains within normal visual line-of-sight of the observer. These aids to vision are not to be confused with corrective lenses or contact lenses, which do not alter the field of view or distort vision.

(3) The responsibility of ensuring the safety of flight and adequate visual range coverage to avoid any potential collisions remains with the PIC. The PIC for each UAS operation must identify a location from which the observer will perform his/her duties. This location will be selected to afford the best available view of the entire area within which the operation is to be conducted.

(4) Daisy-chaining of observers to increase operational distance is not normally approved; however, a proponent may provide a safety case for daisy-chaining in accordance with paragraph 16 by demonstrating an acceptable level of risk to the NAS.

(5) Observer(s) must be in place 30 minutes prior to night operations to ensure dark adaptation. Refer to subparagraph 13.i.(2)(b) for night operations information.

b. ATC Communications Requirements.

(1) The UAS pilot must establish and maintain direct two-way radio communication with appropriate ATC facilities anytime:

- The aircraft is being operated in Class A or D airspace (under §§ 91.135 or 91.129) or, when required, in Class E and G airspace (under §§ 91.127 or 91.126). See subparagraph 13.q.(2) and (3) for operations in Class B or C airspace; or
- The aircraft is being operated under instrument flight rules (IFR); or
- It is stipulated under the provisions of any issued COA or Special Airworthiness Certificate.

(2) It is preferred that communications between the UAS pilot and ATC be established through onboard radio equipment to provide a voice relay, however, for IFR flight this method of transmission is required.

c. Inter-Communications Requirements. Any VO, sensor operator, or other person charged with providing see-and-avoid assistance must have immediate communication with the UAS pilot. If a chase aircraft is being utilized, immediate communication between the chase aircraft and the UAS pilot is required at all times. If the UAS pilot is in communication with ATC, monitoring of the ATC frequency by all UAS crew members (pilots, observers, and chase pilots) is recommended for shared situational and navigational awareness. However, unless it is approved for others to do so, the UAS PIC or the supplemental pilots are the only crewmembers that will communicate with ATC.

d. Electronic Devices. The use of electronic devices (including cell phones) other than for UAS flight- and mission-required usage is governed by § 91.21, which ensures these devices do not interfere with the UAS systems. The use of electronic devices (including cell phones) is not authorized for primary communication with ATC unless authorized under the Special Provisions of the COA.

e. Dropping Objects/Expendable Stores or Hazardous Materials. If the intended UAS operation includes the carriage, dropping, or spraying of aircraft stores outside of active Restricted or Warning Area airspace designated for aviation use, or approved Prohibited Areas, the proponent must ensure that specific approval is listed in the special provisions, the operational risks have been sufficiently mitigated as required by 14 CFR § 91.15, and that the hazardous material requirements in 49 CFR have been met. Acceptable procedures for hung stores and loss of control link while carrying stores must be provided to the FAA. A similar case must be made for hazardous materials carried aboard the aircraft and, if approved, will be listed in the special provision section of the COA.

f. Flight Over Populated Areas. Routine UAS operations are prohibited over urban or populated areas, except where the level of airworthiness allows. UAS operations may be approved in emergency or national disaster relief situations if the proposed mitigation strategies are found to be acceptable. See Appendix A for definition of populated or urban area.

g. Air Shows. A proponent is required to provide a safety case in accordance with paragraph 16 that demonstrates an acceptable level of risk and must receive a separate Air Show Waiver in accordance with FAA Order 8900.1, Flight Standards Information Management System (FSIMS).

h. Flight Over Heavily Trafficked Roads or Open-Air Assembly of People. UAS operations must avoid these areas, except where level of airworthiness allows. If flight in these areas is required, the proponent is required to support proposed mitigations with system safety cases that indicate the operations can be conducted safely. Acceptable system safety cases must include information located in paragraph 16. Additionally, it is the proponent's responsibility to demonstrate that risk of injury to persons or property along the flightpath has been mitigated. UAS with performance characteristics that impede, delay, or divert other air traffic operations may be restricted in their operations. Refer to AC 120-92 and FAA Order 8000.369, current editions.

i. Day/Night Operations.

(1) Day Operations. UAS operations outside of Class A airspace, active Restricted or Warning Areas designated for aviation use, or approved Prohibited Areas will be conducted during daylight hours unless otherwise authorized.

(2) Night Operations.

(a) Night operations may be considered if the proponent provides a safety case and sufficient mitigation to avoid collision hazards at night.

(b) UAS night operations are those operations that occur between the end of evening civil twilight and the beginning of morning civil twilight, as published in the American Air Almanac, converted to local time. (Note: this is equal to approximately 30 minutes after sunset until 30 minutes before sunrise, except in Alaska.) External pilots and observers must be in place 30 minutes prior to night operations to ensure dark adaptation.

j. Flights Below Class A Airspace. All UAS operations outside of active Restricted/ Warning/Sensitive Security Information (SSI) airspace designated for aviation use, or approved Prohibited Areas must be conducted in visual meteorological conditions (VMC) if using ground or airborne VOs. In addition, the following weather requirements apply:

- If on IFR flight, remain clear of clouds. This requirement does not relieve the PIC from following the ATC clearance. According to § 91.3, the PIC retains responsibility for, and is the final authority as to the operation of that aircraft.
- If on VFR flight, maintain § 91.155 VFR cloud clearances, except in Class G airspace, where Class E airspace visibility requirements must be applied, but not less than 3 statute miles (SM) in-flight visibility.
- Special VFR is not permitted.
- For chase aircraft, 5 SM in-flight visibility.

k. Autonomous Operations. Although it is possible to have a completely manual (direct pilot intervention) UAS, the majority of UAS are autonomous to a certain degree. Only those UAS which have the capability of direct pilot intervention will be allowed in the NAS outside of active Restricted or Warning Areas designated for aviation use, or approved Prohibited Areas. Because the pilot may be technically considered out-of-the-loop in a lost link scenario, this restriction does not apply to UAS operating under lost link.

l. Operations from Off-Airport Locations. In most cases, an off-airport location should be situated no closer than 5 nautical miles (NM) from any airport or heliport. The operational areas, including the launch and recovery zones, should be free from obstructions; reasonable efforts should be made to keep operations away from structures.

m. Crew Resource Management (CRM). Proponents must train all UAS crewmembers in CRM. The current edition of FAA AC 120-51, Crew Resource Management Training, or an FAA-recognized equivalent applies to UAS operations. Proponents must implement the recommended training and procedures included in AC 120-51, or in an FAA-recognized

equivalent. The PIC of a UAS must ensure no activities other than those duties required for safe flight operation are performed. No UAS crewmember may engage in any activities unrelated to those required for safe operation of the UAS during critical phases of flight such as launch/takeoff and landing/recovery.

n. Sterile Cockpit. Proponents must comply with the current edition of AC 120-71, Standard Operating Procedures for Flight Deck Crewmembers, or the FAA-recognized equivalent, for ensuring the PIC implements sterile cockpit procedures. During critical phases of flight, including all ground operations involving taxi (movement of an airplane under its own power on the surface of an airport), takeoff and landing, and all other flight operations in which safety or mission accomplishment might be compromised by distractions, no crewmember may perform any duties not required for the safe operation of the aircraft. No crewmember may engage in, nor may any PIC permit, any activity during a critical phase of flight which could distract any crewmember from the performance of his/her duties or interfere in any way with the proper conduct of those duties.

o. Operating Under IFR. While operating on an instrument flight plan, the following must exist, be completed, or be complied with:

(1) The PIC must hold a current instrument rating or an FAA-recognized equivalent.

(2) The aircraft's airworthiness signature statement for flight release (not airworthiness document) must include IFR flight and indicate that all equipment required for IFR operations is certified and working (including pitot-static and transponder checks).

(3) Applicable navigation database and charts are current and available to the UAS pilot.

(4) An IFR flight plan is filed.

(5) An ATC clearance has been obtained and all clearances must be followed.

(6) Direct two-way radio communication between the UAS pilot and ATC is established and maintained. (A communication relay through the aircraft may be required.)

(7) Alternate communication capabilities with ATC for the purpose of lost link and/or lost communication are designated and operational during all phases of flight.

(8) The UAS is equipped with a certified operating mode C (mode S preferred) transponder.

(9) ATC radar services are obtained throughout the portion of the flight in Class A airspace whenever possible (overwater non-radar operations may be allowed in the special provisions section).

(10) All operations outside of Class A airspace and active Restricted, Prohibited, Warning Areas, or SSI airspace designated for aviation use, must remain clear of clouds. If operating under IFR, to comply with this provision, the PIC must have an ATC clearance to deviate.

According to § 91.3, the PIC retains responsibility for, and is the final authority as to, the operation of that aircraft.

(11) VOs are not required in Class A airspace unless stipulated in the COA.

p. Chase Aircraft Operations. The chase aircraft:

(1) Must remain at a safe distance from UA to ensure collision avoidance if a malfunction occurs, and

(2) Must remain close enough to the UA to provide visual detection of any conflicting aircraft and advise the PIC of the situation.

(3) Must remain within radio control range of the UA, in the case of pilot operation from the chase aircraft, to maintain appropriate signal coverage for flight control or activation of the FTS.

(4) May be required to have communication with appropriate ATC facilities based on the proponent's application or mission profile.

(5) Is not required by FAA in active Restricted or Warning Area airspace designated for aviation use, or approved Prohibited airspace.

(6) Is not required for Optionally Piloted Aircraft (OPA) if a qualified VO is on board.

(7) Is not required in Class A airspace unless stipulated in the COA.

(8) Operations must be conducted in accordance with the Special Provisions listed in the approved COA.

(9) Must maintain 5 SM in-flight visibility restrictions.

(10) Pilot/observer:

- Will not concurrently perform either observer or UAS pilot duties along with chase pilot duties unless otherwise authorized.
- Must maintain direct voice communication with the UAS pilot.

(11) Pilots operating as a formation flight will immediately notify ATC if they are using a non-standard formation. Non-standard formations must be pre-approved by ATC. Proponents adhere to the current edition of Order JO 7610.4, Special Operations, as applicable. Refer to Appendix A for definitions of standard and non-standard formations.

(12) Operations will not be conducted in IMC.

(13) Operations will be thoroughly planned and briefed.

(14) Pilot, during a lost link situation, must be notified immediately along with ATC. The chase pilot will report to ATC that the UA is performing lost link procedures as planned or if deviations are occurring.

(15) Pilot will ensure safe separation with the UA, and immediately notify ATC and the UA PIC during loss of visual contact with the UA by both the chase pilot and observer, when such contact cannot be promptly re-established. The UA PIC will either execute lost link procedures to facilitate a rejoin, recover the UA, or terminate the flight as appropriate.

q. Airspace Considerations by Airspace Designation.

Note: UAS operating in airspace designated as reduced vertical separation minimum (RVSM) airspace must comply with § 91.180.

(1) Class A. Observers are not normally required in Class A. All UAS must be operating under IFR and on an instrument flight plan. UAS operations approved for Class A must comply with § 91.135.

(2) Class B. UAS operations are currently not authorized. Class B airspace contains terminal areas with the highest density of manned aircraft in the NAS. On a case-by-case basis, the FAA may consider exceptional circumstances. For public aircraft, a Letter of Agreement (LOA) between the affected ATC facility and the proponent describing UAS segregation procedures is required. For civil aircraft, segregation procedures should be incorporated into the operating limitations. UAS operations must not impede, delay, or divert other Class B operations.

(3) Class C (and airspace within 30 NM of an airport listed in Appendix D, section 1, § 91.215). UAS operations approved for Class C must comply with §§ 91.130 and 91.215. Requests for operations without this equipment will be handled on a case-by-case basis and may be approved if sufficiently mitigated and a safety case has been established. For public aircraft, an LOA between the affected ATC facility and the proponent describing UAS segregation procedures may be required. For civil aircraft, segregation procedures should be incorporated into the operating limitations. UAS operations must not impede, delay, or divert other Class C operations.

(4) Class D. Requests for approval will be handled on a case-by-case basis and may be approved if sufficiently mitigated and a safety case has been established. UAS operations approved for Class D must comply with § 91.129. For public aircraft, an LOA between the affected ATC facility and the proponent describing UAS segregation procedures may be required. For civil aircraft, segregation procedures should be incorporated into the operating limitations. UAS operations must not impede, delay, or divert other Class D operations.

(5) Class E. If there is an operating ATC tower, Class D rules may apply. UAS operations approved for Class E must comply with § 91.127. For public aircraft, an LOA between the affected ATC facility and the proponent describing UAS segregation procedures may be required. For civil aircraft, segregation procedures should be incorporated into the operating limitations. UAS operations must not impede, delay, or divert other Class E operations.

(6) Class G. UAS operations approved for Class G must comply with § 91.126.

r. ATC Visual Approach Clearances. The UAS PIC must not accept a visual approach clearance, an instruction to follow another aircraft by visual means, or a clearance to maintain visual separation from another aircraft.

s. In-Flight Emergencies.

- The PIC will notify ATC of any in-flight emergency or aircraft accident as soon as practical.
- The PIC will notify ATC of any loss of control link as soon as practical. Loss of control link scenarios may be handled by ATC as an emergency.

14. Contingency Planning Limitations. See Appendix E.

15. Personnel Qualifications. This paragraph addresses the qualifications of all UAS flightcrew members, observers, maintainers, and other personnel as appropriate. All references to a pilot certificate or FAA written examination refer to an FAA-issued private pilot certificate, higher certification, or an FAA-recognized equivalent.

a. UAS Pilot Qualifications. The FAA is focused on ensuring that UAS pilots have an appropriate level of understanding of 14 CFR applicable to the airspace where UAS operate. UAS pilots are responsible for controlling their aircraft to the same standards as the pilot of a manned aircraft. Civil UAS pilots may be required to have instruction by an FAA-certificated flight instructor.

b. UAS General Operational Requirements. The following operational restrictions apply to all UAS pilots:

- One PIC must be designated at all times.
- The PIC of an aircraft is directly responsible for, and is the final authority of the operation of that aircraft.
- Pilots must not perform crew duties for more than one UAS at a time.
- Pilots are not allowed to perform concurrent duties both as the pilot and the VO. In the case of OPA, the airborne pilot may assume the role of PIC at all times, but will only be the observer when the OPA is operated by the CS pilot.
- Unless undergoing initial qualification training, pilots must be qualified on the aircraft being flown.
- Only one PIC per aircraft is authorized, and the PIC must be in a position to assume control of the aircraft.

c. PIC.

(1) The designated PIC:

- Has been designated as PIC before or during the flight.
- Is responsible for the UAS flight operation as described under § 91.3, or FAA-recognized equivalent.
- Is responsible for determining whether the UAS is in condition for safe flight.

- Must land as soon as safely practical when any condition occurs that causes operations to be unsafe.
- May be augmented by supplemental pilots; however, the PIC retains complete and overall responsibility of the flight, regardless of who may be piloting the aircraft.
- Has the ability to assume the duties of an internal or an external UAS pilot at any point during the flight.
- May rotate duties as necessary to fulfill operational requirements.
- Operating under a public agency, must have a thorough knowledge of the COA issued to the organization and must retain a copy to reference during flight.
- Must be trained and qualified on the specific UAS for the conduct of the flight.
- May assume the duties of VO or PIC, if piloting an OPA when the OPA is being utilized as a UAS and being flown by the CS pilot.

(2) PIC Rating Requirements. Rating requirements for the UAS PIC depend on the type of operation conducted; they fall into two categories:

- Operations that require at least a private pilot certificate or FAA-recognized equivalent, or
- Operations that do not require at least a private pilot certificate or FAA-recognized equivalent.

(a) The requirement for the PIC to hold a pilot certificate or FAA-recognized equivalent is based on various factors including:

- The location of the planned operations,
- The mission profile,
- The size of the aircraft, and
- Whether or not the operation is conducted within or beyond visual line-of-sight.

(b) The PIC must hold, at a minimum, an FAA private pilot certificate or FAA-recognized equivalent for all operations listed below:

- Flight in Class A, B, C, D, E, and G (400 feet above ground level (AGL)) airspace.
- IFR (must have instrument rating) operations.
- Night operations.
- At joint use or public airfields.
- Requiring a chase aircraft.
- At any time the FAA has determined the need, based on the UAS characteristics, mission profile, or other operational parameters.

(c) Operations without a pilot certificate may be allowed when all of the following conditions are met:

- The PIC has successfully completed, at a minimum, FAA private pilot ground instruction and passed the FAA Private Pilot written examination or FAA-recognized equivalents. (Airman Test Reports are valid for the 24 calendar-month period preceding the month the exam was completed, at which time the instruction and written examination must be repeated.)
- Operations are during daylight hours.
- The operation is conducted in a sparsely populated location.
- Operations are approved and conducted solely within visual line-of-sight in Class G airspace.
- Visual line-of-sight operations are conducted no further than ½ NM laterally from the UAS pilot and at an altitude of no more than 400 feet AGL at all times. Refer to Appendix A for the visual line-of-sight definition.
- Operations are conducted no closer than 5 NM from any FAA-designated airport or heliport other than the airport from which the aircraft is operating.
- The operation is conducted from a privately owned airfield, military installation, or off-airport location.

(3) PIC Recent Flight Experience (Currency). The proponent must provide documentation showing the pilots maintain an appropriate level of recent pilot experience in the UAS being operated, or in an FAA-certified simulator. At a minimum, the PIC must conduct three takeoffs (launch) and three landings (recovery) in the specific UAS within the previous 90 days (excluding pilots who do not conduct launch/recovery during normal/emergency operations); or as prescribed by the proponent's accepted recurrent training and currency program.

(a) For those operations that require a certificated pilot, the PIC, to exercise the privileges of his certificate, must have flight reviews and maintain recent pilot experience in manned aircraft per 14 CFR part 61, as appropriate; or FAA-accepted equivalent.

(b) For flights approved for night operations, the PIC must conduct three takeoffs (launch) and three landings (recovery) each, in the specific UAS at night, to a full stop in the previous 90 days (excluding pilots who do not conduct launch/recovery during normal/emergency operations).

(c) For operations approved for night or IFR, the PIC must maintain recent pilot experience per § 61.57 or FAA-accepted equivalent as applicable.

(4) PIC Medical. The PIC must maintain, at a minimum, a valid FAA second-class medical certificate issued under 14 CFR part 67 or the FAA-recognized equivalent. The second-class medical certificate expires at the end of the last day of the 12th month after the month of the date of the examination shown on the medical certificate listed in § 61.23.

(5) Section 91.17 or FAA-recognized equivalent applies to all UAS crewmembers.

(6) PIC Training.

(a) In addition to the training required for a pilot certificate, UAS PICs must have the following additional training (or FAA-recognized equivalent):

- Including normal, abnormal, and emergency procedures in all specific details of the UAS being operated,
- Manufacturer-specific training,
- Demonstrated proficiency, and
- Testing in the UAS being operated.

(b) Proponents must maintain individual training records of all UAS personnel. All training and testing will be documented in the individual's training record by the instructor and initialed by the trainee.

d. Supplemental Pilots. Supplemental pilots are those pilots assigned UAS flight duty to augment the PIC. It is common for proponents to have both an internal and an external UAS pilot. The supplemental pilot can assume either of these positions.

(1) Ratings. Supplemental pilots must have, at a minimum, successfully completed private pilot ground school and passed the written test or FAA-recognized equivalents. The ground school written test results are valid for two years from the date of completion, at which time the instruction and written examination must be repeated. If a supplemental pilot assumes the role of PIC, he/she must comply with the PIC rating, currency, medical, and training requirements listed above in subparagraph 15c.

(2) Recent Pilot Experience. The proponent must provide a process that ensures that pilots maintain an appropriate level of recent pilot experience for the position they are assigned in the UAS being operated.

(3) Medical. Supplemental pilots must maintain, at a minimum, a valid FAA second-class medical certificate issued under part 67 or the FAA-recognized equivalent. The second-class medical certificate expires at the end of the last day of the 12th month after the month of the date of the examination shown on the medical certificate, according to § 61.23. Section 91.17 or FAA-recognized equivalent applies to all UAS crewmembers.

(4) Training.

(a) UAS supplemental pilots must have:

- Training in all specific details of the UAS being operated, including normal, abnormal, and emergency procedures;
- Manufacturer-specific training (or FAA-recognized equivalent);
- Demonstrated proficiency and successful testing in the UAS being operated.

(b) Proponents must maintain individual training records for all UAS personnel. All training must be documented by the instructor and initialed by the trainee.

e. UAS Observer Qualifications. All observers must have an understanding of Federal aviation regulations applicable to the airspace where the UAS will operate. Observers are considered crewmembers. Observers must not perform crew duties for more than one UAS at a time. Observers are not allowed to perform concurrent duties both as UAS pilot and observer.

(1) Medical. All observers must have a valid FAA second-class medical certificate issued under part 67; an FAA-recognized equivalent is an acceptable means of demonstrating compliance with this requirement. The second-class medical certificate expires at the end of the last day of the 12th month after the month of the date of the examination shown on the medical certificate. Section 91.17 or FAA-recognized equivalent applies to all UAS crewmembers.

(2) Training. Observers must complete sufficient training to communicate to the pilot any information required to remain clear of conflicting traffic, terrain, and obstructions, maintain proper cloud clearances, and provide navigational awareness. This training, at a minimum, must include knowledge of:

(a) Their responsibility to assist pilots in complying with the requirements of 14 CFR:

- § 91.111, Operating Near Other Aircraft;
- § 91.113, Right-of-Way Rules: Except Water Operations;
- § 91.115, Right-of-Way Rules: Water Operations; and
- § 91.155, Basic VFR Weather Minimums;

(b) Air traffic and radio communications, including the use of approved ATC/pilot phraseology; and

(c) Appropriate sections of the Aeronautical Information Manual (AIM).

f. UAS Maintenance Personnel Qualifications.

(1) Maintenance Ratings. Will be established as more data is collected and a regulatory guideline is developed.

(2) Recent Maintenance Experience. It is suggested that proponents follow applicable guidelines of 14 CFR part 65, § 65.83, as appropriate, until final UAS regulatory guidelines are available.

(3) Maintenance Medical Requirements. At a minimum, the requirements of § 91.17 or FAA-recognized equivalent must be met. No additional medical requirements have been defined at this time.

(4) Maintenance Training. It is highly recommended that a proponent of a UAS submit a training program. This requirement will be further defined as more data is collected and the regulatory process affects these guidelines.

g. Other UAS Personnel Qualifications. Ancillary personnel such as systems operators or mission specialists must be thoroughly familiar with and possess operational experience of the equipment being utilized. If the systems being utilized are for observation and detection of other aircraft for collision avoidance purposes, personnel must be thoroughly trained on collision avoidance procedures and techniques and have direct communication with the UAS pilot, observer, and other applicable personnel.

16. AMOC. This notice defines certain limitations and procedures to conduct UAS operations, but each application is evaluated on its own technical merit based on its own set of operational parameters and proposed operational profiles, mitigations, and systems. When a proponent desires to deviate from these limitations and procedures, an AMOC that includes a safety case (recommended format provided in Appendix D), must be submitted for approval. For a proponent to make an acceptable safety case, information must be provided that outlines all hazards and risks associated with the requested AMOC. In addition, the proponent must provide a description of the methods and procedures or equipment for mitigating each hazard and risk. As such, deviations and AMOC may differ from the information presented in this notice. Therefore, if the proponent provides an acceptable safety case with sufficient data that supports the proposal, the AMOC will be considered and evaluated for approval.

a. Safety Case Information. The proponent should include at a minimum:

(1) A thorough description of the environment in which the aircraft will operate;

(2) Criteria for categorizing hazards (e.g., severity and likelihood);

(3) A detailed airworthiness description of the affected items associated with the proposed AMOC, which includes, as a minimum:

- Certification status of components and systems, or statement of airworthiness for public aircraft,
- Reliability data,
- Redundant systems,
- Failure modes and effects, including system response to loss of control link, and
- An airworthiness determination (for COA proponents only);

(4) Capabilities of the aircraft;

(5) Flight data;

(6) Accident data;

(7) Emergency procedures; and

(8) Pilot/crew roles and responsibilities.

b. Sample Safety Case. Appendix D represents the FAA's approach to documenting the process used for hazard identification and risk mitigation. It is provided as an example for proponents to use when developing and documenting a safety case. In addition to these

guidelines, other government and industry methods similar to the FAA's approach to developing a safety case also provide acceptable hazard analysis tools. These include Preliminary Hazard Analysis, Operational Safety Assessment, Comparative Safety Assessment, and Fault Hazard Analysis. See Appendix D for a complete list.

17. Disposition. We will incorporate the information in this notice into FAA Order 8900.1 before this notice expires. Direct questions concerning the information in this notice to the Unmanned Aircraft Systems Integration Office, AFS-80, at 202-385-4835.

for John M. Allen
John M. Allen
Director, Flight Standards Service

APPENDIX A. DEFINITIONS

1. Aircraft. A device used or intended to be used for flight in the air, including unmanned aircraft (UA).

2. Airworthiness [UAS]. A condition in which the unmanned aircraft system (UAS) (including the aircraft, airframe, engine, propeller, accessories, appliances, and control station (CS)) conforms to its type certificate, if applicable, and is in condition for safe operation.

3. Airworthiness Certification. Process and aircraft qualification for civil UAS proponents to obtain a special airworthiness certificate.

4. Airworthiness Statement. Document required from public UAS proponents during a Certificate of Waiver or Authorization (COA) application process which confirms aircraft airworthiness.

5. Certificate of Waiver or Authorization (COA). An FAA grant of approval for a specific operation. The authorization to operate a UAS in the National Airspace System (NAS) as a public aircraft outside of Restricted, Warning, or Prohibited areas approved for aviation activities.

6. Chase Aircraft. A manned aircraft that carries its own pilot-in-command (PIC) and a separate qualified VO flying in proximity to a UA.

7. Civil Aircraft. Aircraft other than public aircraft.

8. Cooperative Aircraft. Aircraft that have an electronic means of identification (i.e., a transponder or ADS-B transceiver) aboard in operation.

9. Crewmember [UAS]. In addition to the crewmembers identified in 14 CFR part 1, a UAS flightcrew member includes pilots, sensor/payload operators, and VOs, but may include other persons as appropriate or required to ensure safe operation of the aircraft.

10. Crew Resource Management (CRM). The effective use of all available resources including human, hardware, and information resources.

11. Daisy-Chaining. Aviation jargon for the use of multiple, successive observers to extend the flight of a UA beyond the direct visual line-of-sight of any other PIC or VO.

12. Experimental Certificate. A type of special airworthiness certificate issued for the purposes of research and development (R&D), crew training, exhibition, and market survey as defined in 14 CFR part 21, § 21.191(a), (c), and (f). Note: According to § 91.319(a)(2), experimental aircraft may not be used for carrying persons or property for compensation or hire.

a. R&D Aircraft. Aircraft testing new design concepts, equipment, installations, operating techniques, or uses for aircraft. Any unmanned aircraft system (UAS), including an Optionally Piloted Aircraft (OPA) is eligible for an experimental certificate under this purpose. Operations

may be conducted by the proponent only as a matter of research or to determine whether an idea warrants further development.

b. Crew Training. Crew training is limited to the number of flight crews required by the proponent to conduct experimental aircraft operations.

c. Market Survey. Aircraft may be used for the purposes of conducting market surveys, sales demonstrations, and customer crew training of the manufacturer's customers as provided in part 21, § 21.195.

13. External Pilot. A UAS pilot who flies from outside a CS shelter with direct visual contact with the aircraft.

14. FAA-Recognized Equivalent. An FAA recognition that a public agency may exercise its own internal processes regarding airworthiness and pilot, aircrew, and maintenance personnel certification and training; furthermore, the agency has determined that its UAS is capable of safe operation in the National Airspace System (NAS) when conducting public aircraft operations under Title 49 of the United States Code (49 U.S.C.) §§ 40102(a)(41) and 40125.

15. Fly-Away. An interruption or loss of the control link, or when the pilot is unable to effect control of the aircraft and, as a result, the UA is not operating in a predicable or planned manner.

16. Formation.

a. Non-standard formation. A formation operating under any of the following conditions:

- When the flight leader has requested and ATC has approved other than standard formation dimensions;
- When operating within an authorized block altitude or under the provisions of a letter of agreement (LOA);
- When the operations are conducted in airspace specifically designed for a special activity.

b. Standard formation. A formation in which proximity of no more than 1 NM laterally or longitudinally and within 100 feet vertically from the flight leader is maintained by each wingman or UA.

17. Inspection. The routine performance of inspection tasks at prescribed intervals. The inspection must ensure the airworthiness of an aircraft up to and including its overhaul or life limits.

18. Internal Pilot. A UAS pilot who flies from inside a CS shelter without direct visual contact with the aircraft.

19. Lost Link. An interruption or loss of the control link, or when the pilot is unable to effect control of the aircraft and, as a result, the UA will perform a predictable or planned maneuver. Loss of command and control link between CS and aircraft. There are two types of links:

- An uplink which transmits command instructions to the aircraft, and
- A downlink which transmits the status of the aircraft and provides situational awareness to the pilot.

20. Missile. A non-recoverable, powered, guided munition that travels through the air or space.

- Ballistic missiles follow a ballistic trajectory.
- Cruise missiles generate lift.
- Guided missiles are launched from a ship or aircraft and serve as a self-contained precision bomb.

21. Non-Cooperative Aircraft. Aircraft that do not have an electronic means of identification (e.g., a transponder) aboard or that have inoperative equipment because of malfunction or deliberate action.

22. Non-Standard Formation. See Formation.

23. Observer. A trained person who assists a UAS pilot in the duties associated with collision avoidance and navigational awareness through electronic or visual means. (Collision avoidance includes, but is not limited to, avoidance of other traffic, clouds, obstructions, terrain and navigational awareness.) A visual observer (VO) is a trained person who assists the UAS pilot by visual means in the duties associated with collision avoidance. A VO includes the OPA pilot when the OPA is being operated as a UAS.

24. Off-Airport. Any location used to launch or recover aircraft that is not considered an airport (e.g., an open field).

25. Optionally Piloted Aircraft (OPA). An aircraft that can conduct operations as a traditional aircraft with a pilot aboard the aircraft, and can also operate as a UAS when the aircraft is operated and controlled by the CS pilot, allowing the pilot aboard the aircraft to become a qualified observer and remain a PIC. OPA operating as a UAS must meet UAS guidance requirements.

26. Pilot Duty Period. The period beginning when a flightcrew member is required to report for duty, with the intention of conducting a flight, and ending when the aircraft is parked after the last flight. It includes the period of time before a flight or between flights that a pilot is working without an intervening rest period.

27. Pilot-in-Command (PIC)-[UAS]. The person who has final authority and responsibility for the operation and safety of flight, has been designated as PIC before or during the flight, and holds the appropriate category, class, and type rating, if appropriate, for the conduct of the flight. The responsibility and authority of the PIC as described by 14 CFR part 91, § 91.3 apply to the UA PIC. The PIC position may rotate duties as necessary with equally qualified pilots. The individual designated as PIC may change during flight. Note: The PIC can only be the PIC for one aircraft at a time. For OPA, PIC must meet UAS guidance requirements for training, pilot licensing, and medical requirements when operating OPA as a UAS.

28. Populated or Urban Areas. Areas depicted in yellow on a Visual Flight Rules (VFR) sectional chart or as determined from other sources.

29. Proponent. A person or agency making an application for a Certificate of Waiver or Authorization (COA).

30. Public Aircraft. An aircraft operated by a governmental entity (including Federal, State, or local governments, and the U.S. Department of Defense (DOD) and its military branches) for certain purposes as described in 49 U.S.C. §§ 40102(a)(41) and 40125. Public aircraft status is determined on an operation by operation basis. See 14 CFR part 1, § 1.1 for a complete definition of a public aircraft.

31. Public Operator. An operator that is classified as government and/or otherwise qualifies for public aircraft operation under 49 U.S.C. §§ 40102(a)(41) and 40125. Not all flights by a public aircraft operator qualify as a public aircraft operation under the statute. Public aircraft operation status is not automatic for flights conducted by a government entity or a contractor to a government entity.

32. Rocket. A powered, unguided munitions (DOD); or an aircraft propelled by ejected expanding gases generated in the engine from self-contained propellants and not dependent on the intake of outside substances. It includes any part which becomes separated during the operation (14 CFR).

33. Safety Risk Management (SRM). A formalized, proactive approach to system safety. SRM is a methodology that ensures hazards are identified, risks are analyzed, assessed, and prioritized; and results are documented for FAA decision-makers to transfer, eliminate, accept, or mitigate risk.

34. Scheduled Maintenance (Routine). The performance of maintenance tasks at prescribed intervals.

35. Segregation. Setting apart from other air traffic operations in the NAS. Segregation is not synonymous with required air traffic separation standards. Therefore, segregation does not prescribe or mandate criteria such as vertical, lateral, or longitudinal distances.

36. Shells. Munitions that are fired from a gun whether guided or not.

37. Smart Bomb. Precision-guided munitions.

38. Standard formation. See formation.

39. Supplemental Pilot. Pilots assigned UAS flight duties to augment the PIC. It is common for proponents to have both an internal and an external UAS pilot. The supplemental pilot can assume either of these positions. The supplemental pilot may also assume duties of the PIC if the specified qualifications are met.

40. Torpedoes. Powered munitions that travel through water.

41. Unmanned Aircraft (UA). A device used or intended to be used for flight in the air that has no onboard pilot. This devise excludes missiles, weapons, or exploding warheads, but includes all classes of airplanes, helicopters, airships, and powered-lift aircraft without an onboard pilot. UA do not include traditional balloons (see 14 CFR part 101), rockets, tethered aircraft and un-powered gliders.

42. Unmanned Aircraft System (UAS). A UA and its associated elements related to safe operations, which may include CSs (ground, ship, or air-based), control links, support equipment, payloads, flight termination systems (FTS), and launch/recovery equipment.

43. Unscheduled Maintenance (Non-Routine). The performance of maintenance tasks when mechanical irregularities occur.

44. Visual Line-of-Sight. Unaided (corrective lenses and/or sunglasses exempted) visual contact between a PIC or a VO and a UAS sufficient to maintain safe operational control of the aircraft, know its location, and be able to scan the airspace in which it is operating to see and avoid other air traffic or objects aloft or on the ground.

APPENDIX B. ACRONYMS

AC	Advisory Circular
AFPD	Air Force Policy Directive
AFS	Flight Standards Service
AGC	Chief Counsel
AGL	Above Ground Level
AIM	Aeronautical Information Manual
AMOC	Alternative Means of Compliance
AR	Army Regulations
ASI	Aviation Safety Inspector
ATCAA	Air Traffic Control Assigned Airspace
ATCSCC	Air Traffic Control System Command Center
ATO	Air Traffic Organization
ATS	Air Traffic Service
AVS	Aviation Safety
CFIT	Controlled Flight Into Terrain
CFR	Code of Federal Regulations
COA	Certificate of Waiver or Authorization
CRM	Crew Resource Management
CS	Control Station
DCP	Divert/Contingency Points
DHS	Department of Homeland Security
DOD	Department of Defense
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FIR	Flight Information Regions
FL	Flight Level
FSIMS	Flight Standards Information Management System
FTP	Flight Termination Point
FTS	Flight Termination System
GCS	Ground Control Station
GHz	Gigahertz
GMF	Government Master File
HQ	Washington Headquarters
IFR	Instrument Flight Rules
LLP	Lost Link Points
LOA	Letter of Agreement
MHz	Megahertz
MSL	Mean Sea Level
NAS	National Airspace System
NASA	National Aeronautics And Space Administration
NAVAIRINST	Naval Air Systems Command Instruction
NM	Nautical Mile
NTIA	National Telecommunications And Information Administration

OPA	Optionally Piloted Aircraft
PIC	Pilot in Command
POC	Point of Contact
R&D	Research and Development
RF	Radio Frequency
RM	Risk Management
RNAV	Area Navigation
RTB	Return to Base
RVSM	Reduced Vertical Separation Minimum
SM	Statute Mile
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
SSI	Sensitive Security Information
STA	Special Temporary Authority
TAS	Traffic Advisory Systems
TC	Type Certificate
TCAS	Traffic Alert and Collision Avoidance Systems
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
U.S.	United States
USC	United States Code
USCBP	U.S. Customs and Border Protection
USCG	U.S. Coast Guard
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions
VO	Visual Observer

APPENDIX C. RELATED REGULATIONS AND PUBLICATIONS

1. Title 14 of the Code of Federal Regulations (CFR).

a. Part 1, Definitions and Abbreviations.

b. Part 21, Certification Procedures for Products and Parts.

- Section 21.191, Experimental certificates.
- Section 21.193, Experimental certificates: general.
- Section 21.195, Experimental certificates: Aircraft to be used for market surveys, sales demonstrations, and customer crew training.
- Section 21.197, Special flight permits.
- Section 21.199, Issue of special flight permits.

c. Part 23, § 23.1309, Equipment, Systems, and Installations.

d. Part 25, § 25.1309, Equipment, Systems, and Installations.

e. Part 61, Certification: Pilots, Flight Instructors, and Ground Instructors.

- Section 61.23, Medical Certificates: Requirement and Duration.
- Section 61.56, Flight Review.
- Section 61.57, Recent Flight Experience: Pilot in Command.
- Section 61.58, Pilot-in-Command Proficiency Check: Operation of an Aircraft that Requires more than one Pilot Flight Crewmember or is Turbojet-Powered.

f. Part 65, § 65.83, Recent Experience Requirements.

g. Part 67, Medical Standards and Certification.

h. Part 91, General Operating and Flight Rules.

- Section 91.3, Responsibility and Authority of the Pilot in Command.
- Section 91.13, Careless or Reckless Operation.
- Section 91.15, Dropping Objects.
- Section 91.17, Alcohol or Drugs.
- Section 91.21, Portable Electronic Devices.
- Section 91.111, Operating Near Other Aircraft.
- Section 91.113, Right-of-Way Rules: Except Water Operations.
- Section 91.115, Right-of-Way Rules: Water Operations.
- Section 91.126, Operating on or in the Vicinity of an Airport in Class G Airspace.
- Section 91.127, Operating on or in the Vicinity of an Airport in Class E Airspace.
- Section 91.129, Operations in Class D Airspace.
- Section 91.130, Operations in Class C Airspace.
- Section 91.135, Operations in Class A Airspace.
- Section 91.155, Basic VFR Weather Minimums.

- Section 91.157, Special VFR Weather Minimums.
- Section 91.180, Operations within Airspace Designated as Reduced Vertical Separation Minimum Airspace.
- Section 91.203, Civil Aircraft: Certifications Required.
- Section 91.215, ATC Transponder and Altitude Reporting Equipment and Use.
- Section 91.319, Aircraft having Experimental Certificates: Operating Limitations.

2. Title 49 of the Code of Federal Regulations (CFR).

a. Chapter I, Subchapter C, Hazardous Materials Regulations.

b. Chapter VIII, Part 830, Notification and Reporting of Aircraft Accidents or Incidents and Overdue Aircraft, and Preservation of Aircraft Wreckage, Mail, Cargo, and Records.

c. Chapter XII, Part 1520, § 1520.5, Sensitive Security Information.

3. Related Publications (current editions).

4. Advisory Circulars (AC).

- AC 00-1.1, Government Aircraft Operations.
- AC 91-57, Model Aircraft Operating Standards.
- AC 120-51, Crew Resource Management Training.
- AC 120-71, Standard Operating Procedures for Flight Deck Crewmembers.
- AC 120-92, Introduction to Safety Management Systems for Air Operators.

5. FAA Notices. N JO 7210.766, Unmanned Aircraft Operations in the National Airspace System (NAS).

6. FAA Orders.

- JO 1000.37, Air Traffic Organization Safety Management System.
- JO 7110.65, Air Traffic Control.
- JO 7210.3, Facility Operation and Administration.
- JO 7400.8, Special Use Airspace.
- JO 7610.4, Special Operations.
- 8000.369, Safety Management System Guidance.
- 8020.11C, Aircraft Accident and Incident Notification, Investigation, and Reporting.
- 8130.34, Airworthiness Certification of Unmanned Aircraft Systems and Optionally Piloted Aircraft.
- 8900.1, Flight Standards Information Management System.

7. Other Documents.

- Title 47 CFR Part 300, National Telecommunications and Information Administration (NTIA) Manual, Chapter 7.11, Use of Frequencies by Certain Experimental Stations.
- Title 49 United States Code (49 U.S.C.) §§ 40102(a)(41), Definitions.

- FAA Air Traffic Organization (ATO) Safety Management System Manual.
- Memorandum of Agreement Concerning the Operation of Department of Defense Unmanned Aircraft Systems in the National Airspace System (DOD-FAA MoA, September 24, 2007).
- Convention on International Civil Aviation ("Chicago Convention"). 7 December 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

APPENDIX D. SAFETY CASE FORMAT

1. **Signature Page.** Include the following information on the signature page:

   - Title: A clear and concise description of the proposed method for AMOC;
   - Originator Information: Originator's name, organization, contact information, etc.;
   - Safety Risk Management Document (SRMD) Information: Safety Case submission date, revision number, etc.

2. **Executive Summary.** The summary should give a general description of the proposed AMOC, including a list of the hazards with associated risk level (high, medium, low) and their corresponding initial and predicted residual risk. Include a high level system description, a summary of how the Safety Case was developed, and what process/method was used to move through the risk assessment process.

3. **Introduction.** Provide a brief reasoning/rationale for the initiative. The scope of the proposed AMOC, whether it is more complex or far-reaching, will determine the need for increased scope and detail of the analysis to be performed.

4. **Section 1.** Current System/System Baseline. Provide a description of the current system or existing procedures as well as the corresponding (operational) system states. If the proposal entails a procedural change, describe the current procedure and its operational environment. If the current system or procedure is unique and has challenges associated with its unique situation, be sure to delineate.

5. **Section 2.** Proposed Change. Provide a description of the proposed change/procedure, identifying which safety parameters are involved.

6. **Section 3.** Safety Risk Management (SRM) Planning and Impacted Organizations. Prior to initiation of the safety analysis, SRM planning is necessary. It is essential to select the appropriate SRM participants, identify the SRM Panel, schedule milestones, and assign tasks and responsibilities. With regard to the organizations that are impacted by the change, describe the method used for collaboration between those organizations during the identification, mitigation, tracking, and monitoring of hazards associated with the change.

7. **Section 4.** Assumptions. If in the process of developing a procedure to validate an AMOC, any assumptions are made to make the evaluation of the change more manageable, clearly define and document them in this section.

8. **Section 5.** Phase 1: System Description. The description of the system/procedure, its operational environment, the people involved/affected by the change/procedure, and the equipment required to accommodate the proposal must be provided.

9. **Section 6.** Phase 2: Identified Hazards. The SRM Panel identifies hazards as a collaborative effort. The tool(s) and technique(s) used to identify hazards should be specified and discussed. The identified hazards are documented as well as their corresponding causes, the corresponding system states considered and the consequent potential outcome. It is important to realize that while identification of the worst credible outcome and the system state in which the worst

credible outcome occurs is required, system states with less severe outcomes should not be ignored.

10. Section 7. Phase 3 & 4: Risk Analysis & Risks Assessed. Describe the process used to analyze the risks associated with the identified hazards. Specify what type of data was used to determine the likelihood of risk occurrence (e.g., quantitative or qualitative) as well as the sources of the data. A risk matrix should provide an illustration of the predicted initial/current risk(s) associated with the identified hazards.

11. Section 8. Phase 5: Treatment of Risks/Mitigation of Hazards. If the existing controls and mitigations do not acceptably mitigate the hazards, then additional recommended safety requirements should be identified. An explanation of how the recommended safety requirements are expected to reduce the initial/current risk to an acceptable predicted residual risk level should be included. Low-risk hazards may still warrant recommended safety requirements.

12. Section 9. Tracking and Monitoring of Hazards. Once the proposal has been approved and implemented, tracking of hazards and verification of the effectiveness of mitigation controls throughout the lifecycle of the system or change are required. Also, the methodology for this tracking and monitoring should be outlined.

13. Appendices.

a. Documents Related to the SRMD. Include a list of documents (orders, directives, regulations, handbooks, and manuals) that pertain to the proposed change, which have been consulted in the development of the proposed change and the corresponding safety analysis.

b. Hazard Identification Tools. Provide information on the different tool(s), method(s), and technique(s) used during the safety analysis. (See Figure D-1, for a chart listing acceptable hazard analysis tools and techniques.)

c. Hazard Analysis and Risk Matrix. Depending on the analyses necessary, there might be one or more appendices with analyses. A risk matrix reflecting the initial and predicted residual risks should also be included.

d. Glossary. Include any acronyms and definitions for any terms you listed in the Safety Case.

Figure D-1. Acceptable Hazard Analysis Tools and Techniques

This chart from the ATO Safety Management System Manual, available on the Internet, displays acceptable hazard analysis tools for developing safety cases.

Air Traffic Organization Safety Management System Manual - Version 2.1

Table 3.1: Selection of Hazard Identification and Analysis Tools and Techniques

Tool or Technique	Summary Description	Page in Appendix G
Preliminary Hazard Analysis (PHA)	The PHA provides an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not deep.	G-1
Operational Safety Assessment (OSA)	The OSA is a development tool based on the assessment of hazard severity. It establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced.	G-3
Comparative Safety Assessment (CSA)	The CSA provides management with a listing of all of the hazards associated with a change, along with a risk assessment for each alternative hazard combination that is considered. It is used to rank the options for decision-making purposes. The CSA's broad scope is an excellent way to identify issues that may require more detailed hazard identification tools.	G-5
Fault Hazard Analysis (FHA)	The FHA is a deductive method of analysis that personnel can use exclusively as a qualitative analysis or, if desired, can expand to a quantitative one. The FHA requires a detailed investigation of the subsystems to determine component hazard modes, causes of these hazards, and resultant effects on the subsystem and its operation.	G-8
Failure Mode and Effect Analysis (FMEA)	The FMEA determines the results or effects of sub-element failures on a system operation and classifies each potential failure according to its severity.	G-9
Failure Modes, Effects, and Criticality Analysis (FMECA)	The FMECA is an essential function in design from concept through development. To be effective, the FMECA is iterative to correspond with the nature of the design process itself. The FMECA identifies component and sub-system failure modes, including the impact of human error; evaluates the results of the failure modes; determines rates and probability; and demonstrates compliance with safety requirements.	G-9
What-If Analysis	The What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. One can use the What-If Analysis as a brainstorming method.	G-10
Scenario Analysis	The Scenario Analysis identifies and corrects potentially hazardous situations by postulating accident scenarios in cases where it is credible and physically logical.	G-12
Change Analysis	The Change Analysis analyzes the hazard implications of either planned or incremental changes (e.g., operation, equipment, or procedure).	G-13
Cause-Consequence Analysis	The Cause-Consequence Analysis combines the bottom-up and top-down analysis techniques of Event Trees and Fault Trees. The result is the development of potential complex accident scenarios.	G-15

Figure D-1. Acceptable Hazard Analysis Tools and Techniques, continued

Air Traffic Organization Safety Management System Manual - Version 2.1

Tool or Technique	Summary Description	Page in Appendix G
Hazard and Operability Tool (HAZOP)	A group uses the HAZOP to analyze hazards of completely new operations and to review the significance of all of the ways that a process element can malfunction or be incorrectly operated. The technique is essentially a structured brainstorming using specific guide words.	G-17
Interface Analysis	One uses the Interface Analysis to discover the hazardous linkages between interfacing systems.	G-18
Accident/Incident Analysis	The Accident/Incident Analysis uses data on recorded hazardous events. One groups these events in various ways according to a pre-established criterion, usually a common cause or outcome. One then identifies the groupings as hazards.	G-19
Job Safety Analysis (JSA)	One uses this technique to assess in detail the safety considerations in a single job or task..	G-20
Energy Trace and Barrier Analysis (ETBA)	The ETBA is highly structured. It documents all energy sources in system. One identifies the energy sources as hazards. One identifies the barrier between the energy sources and the operators, maintainers, and other systems as mitigations.	G-21
Fault Tree Analysis (FTA)	An FTA is a graphical design technique that can provide an alternative to block diagrams. It is a top-down, deductive approach structured in terms of events. One models faults in terms of failures, anomalies, malfunctions, and human errors.	G-22
Management Oversight and Risk Tree (MORT)	One uses the MORT technique to systematically analyze hazards to examine and determine detailed information about the process and accident contributors.	G-24
Human Error Analysis (HEA)	HEA, in a system context, involves assessing each human-machine interface point, decision, or action for the potential for human error to adversely impact system performance or safety of the system and its users. There are a variety of methodologies for conducting these analyses.	G-26
Job Task Analyses (JTA)	The foundation of the performance of HEA is a task analysis, which describes each human task/sub-task within a system in terms of the perceptual (information intake), cognitive (information processing and decision making), and manual (motor) behaviors required of an operator, maintainer, or support person. It should also identify the skills and information required to complete the tasks; equipment requirements; the task setting; time and accuracy requirements; and the probable human errors and consequences of these errors. There are several tools and techniques for performing task analyses, depending on the level of analysis needed.	G-28

APPENDIX E. CONTINGENCY PLANNING LIMITATIONS

1. Point Identification. The proponent must submit contingency plans that address emergency recovery or flight termination of the unmanned aircraft (UA) in the event of unrecoverable system failure. These procedures will normally include Lost Link Points (LLP), Divert/Contingency Points (DCP) and Flight Termination Points (FTP) for each operation. LLPs and DCPs must be submitted in latitude/longitude (Lat/Long) format along with a graphic representation plotted on an aviation sectional chart (or similar format). FTPs or other accepted contingency planning measures must also be submitted in Lat/Long format along with a graphic representation plotted on an aviation sectional chart, or other graphic representation acceptable to the FAA. The FAA accepts the LLPs, DCPs, FTPs, and other contingency planning measures submitted by the proponent, but does not approve them. When conditions preclude the use of FTPs, the proponent must submit other contingency planning options for consideration and acceptance. At least one LLP, DCP, and FTP (or an acceptable alternative contingency planning measure) is required for each operation. The proponent must furnish this data with the initial Certification of Waiver or Authorization (COA) application. Any subsequent changes or modifications to this data must be provided to the Unmanned Aircraft Systems (UAS) Integration Office (AFS-80) for review and consideration no later than 30 days prior to proposed flight operations.

2. Risk Mitigation Plans. For all operations, the proponent must develop detailed plans to mitigate the risk of collision with other aircraft and the risk posed to persons and property on the ground in the event the UAS experiences a lost link, needs to divert, or the flight needs to be terminated. The proponent must take into consideration all airspace constructs and minimize risk to other aircraft by avoiding published airways, military training routes, Navigational Aids (NAVAIDS), and congested areas. In the event of a contingency divert or flight termination, the use of a chase aircraft is preferred when the UAS is operated outside of Restricted or Warning Areas. If time permits, the proponent should make every attempt to utilize a chase aircraft to monitor the aircraft to a DCP or to the FTP. In the event of a contingency divert or flight termination, the proponent will operate in Class A airspace and Special Use airspace to the maximum extent possible to reduce the risk of collision with non-participating air traffic.

a. LLP Procedures.

(1) LLPs are defined as a point, or sequence of points, where the aircraft will proceed and hold at a specified altitude, for a specified period of time, in the event the command and control link to the aircraft is lost. The aircraft will autonomously hold, or loiter, at the LLP until the communication link with the aircraft is restored or the specified time elapses. If the time period elapses, the aircraft may autoland, proceed to another LLP in an attempt to regain the communication link, or proceed to an FTP for flight termination. LLPs may be used as FTPs. In this case, the aircraft may loiter at the LLP/FTP until link is re-established or fuel exhaustion occurs.

(2) For areas where multiple or concurrent UAS operations are authorized in the same operational area, a segregation plan must be in place in the event of a simultaneous lost link scenario. The deconfliction plan may include altitude offsets and horizontal separation by using independent LLPs whenever possible.

b. DCP Procedures.

(1) A DCP is defined as an alternate landing/recovery site to be used in the event of an abnormal condition that requires a precautionary landing. Each DCP must incorporate the means of communication with air traffic control (ATC) throughout the descent and landing (unless otherwise specified in the Special Provisions) as well as a plan for ground operations and securing/parking the aircraft on the ground. This includes the availability of control stations (CS) capable of launch/recovery, communication equipment, and an adequate power source to operate all required equipment.

(2) For local operations, the DCP specified will normally be the airport/facility used for launch and recovery; however, the proponent may specify additional DCPs as alternates.

(3) For transit and/or mission operations that are being conducted in Class A airspace or Class E airspace above flight level (FL) 600, DCPs will be identified during the flight to be no further than one hour of flight time at any given time, taking into consideration altitude, winds, fuel consumption, and other factors. If it is not possible to define DCPs along the entire flight plan route, the proponent must identify qualified FTPs along the entire route and be prepared to execute flight termination at one of the specified FTPs if a return to base (RTB) is not possible.

(4) It is preferred that specified DCPs are non-joint use military airfields, other government-owned airfields, or private-use airfields. However, the proponent may designate any suitable airfield for review and consideration.

c. Flight Termination Procedures.

(1) Flight termination is the intentional and deliberate process of performing controlled flight into terrain (CFIT). Flight termination must be executed in the event that all contingencies have been exhausted and further flight of the aircraft cannot be safely achieved or other potential hazards exist that require immediate discontinuation of flight. FTPs or alternative contingency planning measures must be located within power-off glide distance of the aircraft during all phases of flight and must be submitted for review and acceptance. The proponent must ensure sufficient FTPs or other contingency plan measures are defined to accommodate flight termination at any given point along the route of flight. The location of these points is based on the assumption of an unrecoverable system failure and must take into consideration altitude, winds, and other factors.

(2) Unless otherwise authorized, FTPs must be located in sparsely populated areas. Except for on- or near-airport operations, FTPs will be located no closer than five nautical miles (NM) from any airport, heliport, airfield, NAVAID, airway, populated area, major roadway, oil rig, power plant, or any other infrastructure. For offshore locations, the proponent must refer to appropriate United States Coast Guard (USCG) charts and other publications to avoid maritime obstructions, shipping lanes, and other hazards. Populated areas are defined as those areas depicted in yellow on a Visual Flight Rules (VFR) sectional chart or as determined from other sources.

(a) It is preferred that flight termination occurs in Restricted or Warning Areas, government-owned land, or offshore locations that are restricted from routine civil use. However, the proponent may designate any suitable location for review and consideration.

(b) The proponent is required to survey all designated areas prior to their use as an FTP. All FTPs will be reviewed for suitability on a routine and periodic basis, not to exceed six months. The proponent assumes full risk and all liability associated with the selection and use of any designated FTP.

(c) It is desirable that the proponent receive prior permission from the land owner or using agency prior to designation of this area as an FTP. The proponent should clearly communicate the purpose and intent of the FTP.

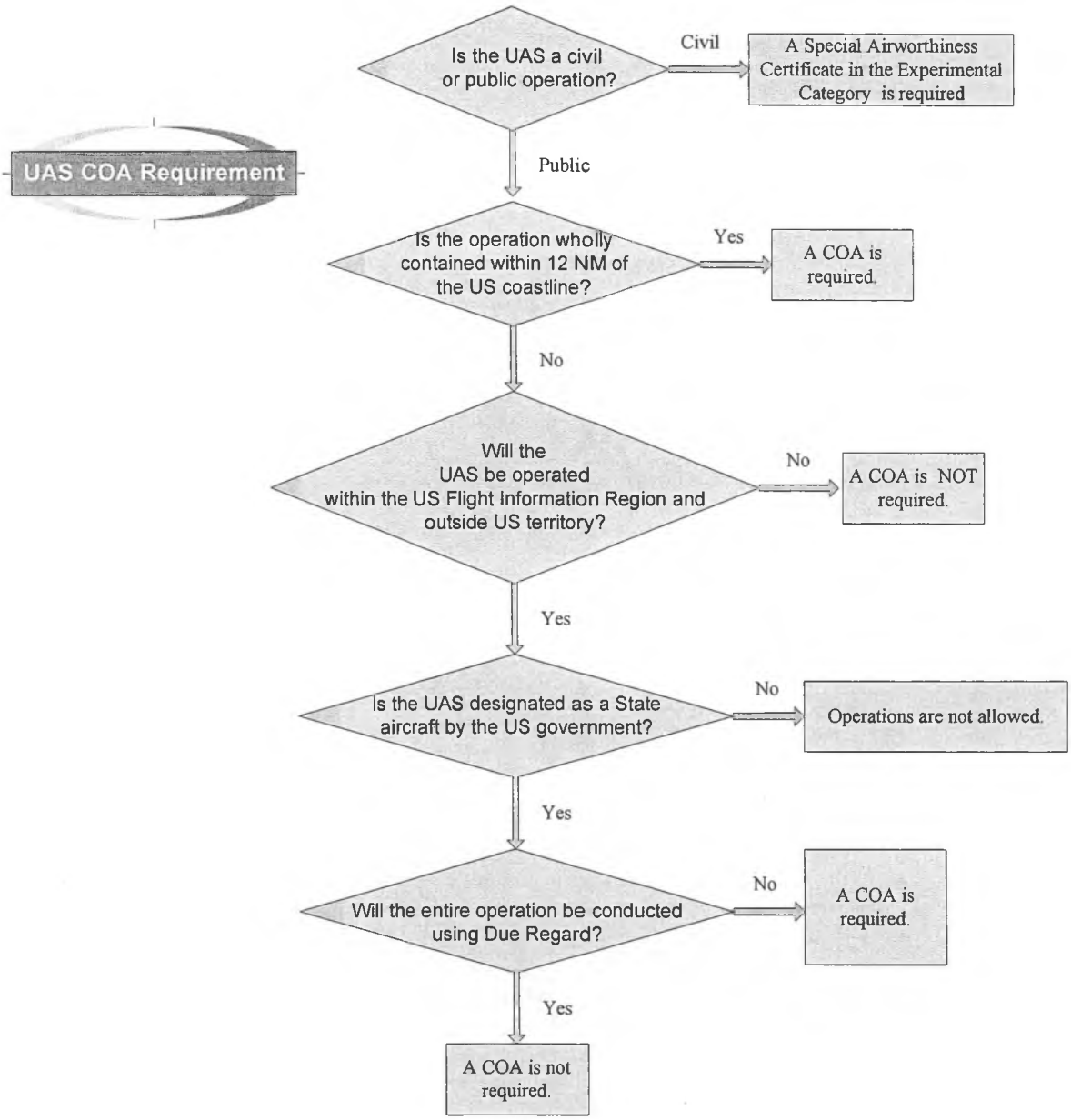
(d) For each FTP, plans must incorporate the means of communication with ATC throughout the descent as well as a plan for retrieval/recovery of the aircraft.

(e) Contingency planning must take into consideration all airspace constructs and minimize risk to other aircraft by avoiding published airways, military training routes, NAVAIDS, and congested areas to the maximum extent possible.

(f) In the event of a contingency divert or flight termination, if time permits, the use of a chase aircraft is preferred when the UA is operated outside of Restricted or Warning Areas.

(g) In the event of a contingency divert or flight termination or other approved contingency measures, the proponent will operate in Class A airspace and Special Use airspace to the maximum extent possible to reduce the risk of collision with non-participating air traffic.

APPENDIX F. UAS COA REQUIREMENT FLOWCHART



LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM September 30, 2013

SUBJECT: Alaska Laws Protecting Privacy
(Work Order No. 28-LS0990)

TO: Representative Shelley Hughes
Attn: Ginger Blaisdell

FROM: Kathleen Strasbaugh
Legislative Counsel

You have asked for a review of Alaska's laws protecting individual privacy in preparation for a meeting of the Task Force on Unmanned Aircraft Systems. Among the Task Force's duties is providing written recommendations concerning, among other things, a state policy that protects privacy. 2013 Legislative Resolve No. 17 at 3. To that end, as I understand from Ms. Blaisdell, you would like to know what protections might already exist, with a view toward avoiding duplication of existing law. The Task Force has apparently expressed concern about how information gathered by unmanned aircraft could be used by private or public parties, and what use might be made of such information captured inadvertently.

This memo will outline constitutionally based protections of privacy and identify state statutes that might apply to conduct considered invasion of privacy. As you requested, this memo focuses on the protections afforded under Alaska law. A brief discussion of emerging federal law is included, but I haven't explored other states' case law, nor lower federal court cases that consider these issues. However, I have attached an excerpt of an *Alaska Law Review* which summarizes Alaska's privacy law as it has developed independently of federal constitutional law. I have also attached a recent *Harvard Law Review* article that specifically addresses this topic in great detail. The memo also briefly addresses scenarios set out in your request. Please note that it is very difficult to predict the outcome of litigation in this very new intersection of technology and privacy law.

1. Constitutional Protection of Privacy

The Constitution of the State of Alaska explicitly protects the right of privacy against government (but not private) intrusion. Art. I, sec. 22, provides:

> The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.

This protection, although not unlimited, has been held to be broader than the protection afforded by the United States Constitution. *Woods & Rohde, Inc. v. State, Department of Labor*, 565 P.2d 138, 149 (Alaska 1977).[1] Both the Alaska Constitution and the Fourth Amendment to the United States Constitution require a warrant by a governmental agency for the search of a place where a person has a reasonable expectation of privacy. *Beltz v. State*, 221 P.3d 328, 333, 337 (Alaska 2009) (search of garbage placed out on the street for collection did not require warrant; expectation of privacy found not reasonable.)

Neither the Alaska Supreme Court nor the United States Supreme Court has ruled on whether surveillance by a government operated unmanned aerial vehicle is a search under the Fourth Amendment. Based on available precedent, it is possible that the courts will decide that the use of an unmanned aerial vehicle constitutes a search requiring either a warrant, or the application of a recognized exception to the warrant requirement.

The United States Supreme Court has considered law enforcement or other government agency use of aerial surveillance and the use of technological devices for surveillance purposes. The Court found that surveillance by manned aircraft is not an intrusion into a private area that renders an overflight a search under the Fourth Amendment to the United States Constitution; however the placement of a global positioning device on a person's vehicle is an intrusion that constitutes a search. Here is a brief summary of some of these cases: *United States v. Jones*, 565 U.S. ___, 132 S.Ct. 945 (2012): Attachment of global positioning device to automobile parked in public place is a search under the Fourth Amendment.

Dow Chemical Co. v. United States, 476 U.S. 227 (1986) EPA aerial surveillance and photography of chemical plant is not a search where the aircraft was manned and operating at a lawful altitude.

California v. Ciraolo, 476 U.S. 207 (1986) Manned aerial surveillance of a backyard marijuana grow at lawful altitude did not violate the Fourth Amendment.

The Court might find the use of a technology that exceeds human observational capacity the sort of intrusion that constitutes a search requiring a warrant or an accepted exception:

> Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.

Kyllo v. United States, 533 U.S. 27, 40 (2001) (internal citations omitted) (thermal

---

[1] In Alaska, the right to privacy extends to protection of such activities as possession and use of marijuana in the home by an adult, which, while not a fundamental right, is protected because such possession and use does not implicate the public welfare in the manner that more harmful substances, or public ingestion, or use by minors might. *Ravin v. State*, 537 P.2d 494, 508-09 (Alaska 1975).

imaging of home from outside a search under the Fourth Amendment).

2. Alaska Statutory protections

There are a handful of criminal statutes that may apply to improper use of images obtained from unmanned aerial vehicle surveillance. These statutes would seem to apply for the most part to private actors. These are offenses that punish conduct that invades the privacy of a victim, and would require proof that images gathered by the unmanned aerial vehicle were disseminated. These offenses would probably not punish capturing the images inadvertently, although collecting and storing them might be a concern.

Alaska Statute	**Charge**	**Penalty**
11.41.270	Stalking in the second degree: nonconsensual conduct prohibited by statute prohibits monitoring by technical means.	Class A misdemeanor[2]
11.61.116	Sending an explicit image of a minor.	(1) class B misdemeanor if the person distributes the image to another person;[3] (2) a class A misdemeanor if the person distributes the image to an Internet website that is accessible to the public.
11.61.120(a)(6)	Harassment in the second degree: publishing or distributing images that show certain body parts or a sexual act.	Class B misdemeanor

[2] A class A misdemeanor is punishable by a fine of up to $10,000, and a sentence of imprisonment up to one year.

[3] A class B misdemeanor is punishable by a fine of up to $2,000, and a sentence of imprisonment up to 90 days.

11.61.123	Indecent viewing or photography (with certain law enforcement and security surveillance exceptions).	(1) class C felony if the person viewed or shown in a picture was, at the time of the viewing or production of the picture, a minor;[4] (2) class A misdemeanor if the person viewed or shown in the picture was, at the time of viewing or production of the picture, an adult.
11.76.113	Misconduct involving confidential information in the first degree: use of confidential information to commit a crime or obtain a benefit to which the person is not entitled to injure another, or deprive another of a benefit.	Class A misdemeanor
11.76.115	Misconduct involving confidential information in the second degree: knowingly and without legal authority obtaining confidential information about another.	Class B misdemeanor

In addition to the above criminal offenses, there are other provisions of law that might bear on the information obtained from data gathered by an unmanned aerial vehicles.

If the data is gathered by a government agency, it is a public record. However, AS 40.25.120 provides certain protections for private information. AS 40.25.120(a)(4) excepts records required by law to be kept confidential. *See Falcon v. APOC*, 570 P.2d 469 (Alaska 1977) (physician not required to disclose identity of certain patients to Alaska Public Offices Commission where the disclosure of the patients' identities might disclose the fact that they were being treated for conditions that patients would normally keep private); *Alaska Wildlife Alliance v. Rue*, 948 P.2d 976 (Alaska 1997) (payroll information may be kept private where disclosure might endanger employees or contractors, where those employees and contractors were threatened with harm). AS 40.25.120(a)(6)(C) protects information gathered by law enforcement the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of the personal privacy of a suspect, defendant, victim, or witness."

---

[4] A Class C felony is punishable by a fine of up to $50,000, and a sentence of imprisonment up to five years. Presumptive sentences based on whether the offense is a first or subsequent offense are set out at AS 12.55.155(e).

There may be civil liability for obtaining (and subsequently misappropriating) information on trade secrets or patented processes. *See, generally.* AS 45.50.

In addition, a person who is subject to surveillance that is unreasonable or unlawful could sue for the tort of invasion of privacy. *Compare Wal-Mart v. Stewart*, 990 P.2d 626, 634 (Alaska 1999) (daily search of employee's bags held an unreasonable invasion of privacy where not part of a random, nondiscriminatory policy, and where the employee feared that refusing the search might result in others suspecting him of theft, or result in a police call or firing).

3. Particular scenarios

Inadvertent capture of evidence of illegal activity. Use of inadvertently captured information in a criminal prosecution may depend on who captures the information, and whether the person whose actions have been captured has a reasonable expectation of privacy. One of the scenarios mentioned in your request is the capture of evidence of poaching. Assuming that the poacher is a person taking game on property that is not the poacher's own, the poacher cannot reasonably expect privacy when present on another's land without authority.

If a law enforcement agency sends out an unmanned aerial vehicle for patrolling or surveillance, perhaps to look for illegal cultivation of marijuana or manufacture of methamphetamine on public land, and in the course of doing so, captures evidence of an industrial sized marijuana grow operation on private land, it might provide grounds to obtain a warrant to explore further.[5] Under Alaska law, if the observation of the event is lawful or in "plain view," the discovery inadvertent, and the incriminating nature of the evidence immediately apparent, a warrant might not be required. *Ahvakana v. State*, 283 P.3d 1284, 1288 (Alaska Ct. App. 2012) (entry into property where evidence found was authorized under the emergency aid exception to the warrant requirement). However, since the vehicle is not manned, the federal authorities discussed above suggest that the information might not be considered to be lawfully obtained unless some other exception to the requirement of a warrant is present. It is not clear to me whether and under what circumstances a court might grant a search warrant to follow up on information inadvertently obtained, but not in "plain view."

It is possible that the inadvertent capture of information that might otherwise be inadmissible under the exclusionary rule that bars admission of evidence obtained in violation of the United States Constitution will be treated as a good faith exception under *United States v. Leon*, 468 U.S. 897(1984). In *Leon*, the United States Supreme Court held that the Fourth Amendment exclusionary rule should not be applied so as to bar the use of evidence obtained by officers acting in reasonable reliance on a search warrant

---

[5] *But see State v. Crocker*, 97 P.3d 93 (Alaska Ct. App. 2004) holding that because the application for the warrant did not affirmatively disclose information that the marijuana cultivation was beyond what was permitted under *Ravin*, there was no probable cause for a warrant.

issued by a detached and neutral magistrate but ultimately found to be invalid. A court could determine that information inadvertently captured in otherwise lawful surveillance is likewise a good faith exception. However, Alaska's appellate courts have not decided whether to adopt this exception. *Deemer v. State*, 244 P.3d 69, 72 (Alaska Ct. App. 2010). Thus it is impossible to predict the outcome of litigation on this subject under Alaska law, and it is not at all clear, given the federal case law developments discussed elsewhere in this memorandum, that the United States Supreme Court would apply the exception in a situation where there was no warrant.

Person intentionally gathers private information for personal use or distribution. A number of the criminal charges listed above might be available. In addition, if the images obtained are used in child pornography, a number of federal and state criminal statutes might apply.

Please advise if you require further assistance in this matter.

KJS:ray
13-008.ray

Enclosures

OBSERVATIONS FROM ABOVE: UNMANNED AIRCRAFT SYSTEMS AND PRIVACY

JOHN VILLASENOR*

INTRODUCTION 458
I. UNMANNED AIRCRAFT SYSTEMS TECHNOLOGY 461
A. Historical Context: The Nineteenth and Twentieth Centuries 462
B. Unmanned Aircraft Systems Today 464
II. REGULATORY FRAMEWORK 468
A. The Federal Aviation Administration 468
B. The FAA and Unmanned Aircraft Systems 470
C. The Impact of Safety Regulations on Privacy 473
III. GOVERNMENT UNMANNED AIRCRAFT AND THE FOURTH AMENDMENT 475
A. *Dow Chemical Co. v. United States* 476
B. *California v. Ciraolo* 477
C. *Florida v. Riley* 480
D. *Kyllo v. United States* 482
E. *United States v. Jones* 484
F. Privacy and Unmanned Aircraft Systems in Light of Supreme Court Jurisprudence 486
1. Technology in "General Public Use" ... 487
2. "Public Navigable Airspace" 489
3. The Role of Imaging Technology 493

---

* Nonresident senior fellow in Governance Studies and the Center for Technology Innovation, the Brookings Institution; Professor of Electrical Engineering, University of California, Los Angeles. The author gratefully acknowledges the assistance of the Association for Unmanned Vehicle Systems International (AUVSI), Thomas Cifarelli, Catherine Crump, and Rich Hanson and Michael Smith of the Academy of Model Aeronautics.

4. Extended Surveillance Using Unmanned Aircraft in Light of *Jones* 495
5. Residual Privacy Rights When a Warrant Is Obtained? 498
IV. NON-GOVERNMENT UNMANNED AIRCRAFT AND THE FIRST AMENDMENT 498
A. Trespassing 499
B. Invasion of Privacy 500
1. Intrusion Upon Seclusion 501
2. Publication of Private Facts 503
C. Stalking and Harassment 505
D. Unmanned Aircraft and Business Privacy 506
V. NEW FRAMEWORKS FOR UNMANNED AIRCRAFT SYSTEMS AND PRIVACY 508
A. Voluntary Approaches 508
B. Federal Legislation 509
C. State and Local Legislation and the Scope of Federal Preemption 513
CONCLUSION 516

INTRODUCTION

Military aviation experts and model airplane hobbyists have known for decades that an airplane can be flown without a human in the cockpit. Until very recently, however, for most people the very concept of an aircraft was inextricably tied to that of the pilot it was presumed to carry. In the long run, that may turn out to be a historical aberration.

"Drones"—more accurately, unmanned aircraft—will dominate the future of aviation as thoroughly as manned aircraft have dominated its past. In the military the transition is well under way. In 2012, the United States military had close to 6,300 unmanned aircraft systems (UAS)[1] and is training hundreds of

1. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS, DEPARTMENT OF DEFENSE REPORT TO CONGRESS ON FUTURE UNMANNED AIRCRAFT SYSTEMS TRAINING, OPERATIONS, AND SUSTAINABILITY 2 (2012), *available at* http://www.fas.org/irp/program/collect/uas-future.pdf. The

new pilots each year to fly them.[2] Civilian UAS use in the United States is also set to grow rapidly in the wake of a law enacted in February 2012 providing for the integration of unmanned aircraft into the national airspace over the next several years.[3]

UAS can be employed in an endless variety of civilian applications, the overwhelming majority of them beneficial. They can be used, for example, to help rescuers identify people in need of assistance following a natural disaster, or to provide vital overhead imagery to police officers attempting to defuse a hostage standoff. In the commercial world, UAS will be increasingly employed for tasks as diverse as surveying, crop spraying, and traffic congestion monitoring. Scientific applications include air quality assessment, wildlife tracking, and measuring the internal dynamics of violent storms. UAS will also generate a number of economic benefits, both by creating jobs that involve the design and production of UAS and by spurring advances in robotics that will apply well beyond aviation, in fields ranging from manufacturing to surgery.

However, like any technology, UAS can be misused. The most common concern regarding domestic UAS relates to their potential impact on privacy. This is a legitimate concern. Existing laws and jurisprudence provide an important foundation, but they also leave many questions unanswered. And although in some respects UAS simply represent one more manifestation of the always complex intersection between technology and privacy, they are also unique in making it possible, for the first time ever, to easily and inexpensively obtain observations from above.

As Justice Samuel Alito wrote in a concurrence in *United States v. Jones*, the January 2012 Supreme Court ruling that addressed the constitutionality of affixing a GPS tracking device

---

term unmanned aircraft system (UAS) refers to an unmanned aircraft as well as the associated communication and control components used in its operation. FAA Modernization and Reform Act of 2012 (FMRA), Pub. L. No. 112-95, § 331, 126 Stat. 11, 72 (2012). "UAS" is also sometimes expanded as "unmanned aerial system." The term unmanned aerial vehicle (UAV) refers to the aircraft itself. *See, e.g.*, Bart Elias, Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System 1 n. 1 (2012), *available at* http://www.fas.org/sgp/crs/natsec/R42718.pdf.

2. Elisabeth Bumiller, *A Day Job Waiting for a Kill Shot a World Away*, N.Y. TIMES, July 29, 2012, http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html.

3. *See* FMRA §§ 331–336, 126 Stat. at 72–78.

to a vehicle without a valid warrant, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."[4] Although Justice Alito's statement was directed toward GPS tracking, it has direct relevance to UAS. In comparison with manned aircraft, UAS can be very inexpensive to procure and operate. As the practical barriers to obtaining aerial imagery fall away, the resulting privacy issues take on heightened importance.

This Article considers the constitutional, statutory, and common law frameworks that will inform privacy rights with respect to observations from unmanned aircraft.[5] The potential privacy challenges raised by unmanned aircraft are direct consequences of their capabilities and of the rules governing the manner in which they can be flown. Accordingly, Part I provides the historical context for UAS technology and describes the range of platforms available today. Part II addresses the current regulatory environment in the United States, with particular attention to those provisions of the FAA Modernization and Reform Act of 2012 (FMRA) that relate to UAS.

Part III discusses government operation of unmanned aircraft in light of the Supreme Court's Fourth Amendment jurisprudence. Although the Supreme Court has never specifically ruled on the question of UAS privacy, it has examined the Fourth Amendment implications of aerial surveillance on several occasions. Part III examines those cases in some detail, as well as *Jones*[6] and *Kyllo v. United States*,[7] and the interpretations they suggest with respect to the constitutionality of UAS observations.

Part IV addresses UAS operated by private entities, who are unconstrained by the Fourth Amendment restrictions that apply to the government. Private UAS users will enjoy strong First Amendment protections for gathering information in public spaces. But the rights conferred by the First Amendment are not unbounded, and it does not take much imagination to conclude

---

4. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment).

5. For another treatment of some of the issues discussed here, see generally ALISSA M. DOLAN & RICHARD M. THOMPSON, II, INTEGRATION OF DRONES INTO DOMESTIC AIRSPACE: SELECTED LEGAL ISSUES (2013), *available at* http://www.fas.org/sgp/crs/natsec/R42940.pdf. Dolan and Thompson's report was released while this Article was in the process of revision for publication.

6. *Id.* at 945.

7. 533 U.S. 27 (2001).

that paparazzi, stalkers, and others could employ UAS in manners that pose clear violations of privacy. Part IV then explores some of the laws that can be used to address such behavior. Part V considers potential new voluntary and statutory privacy solutions and discusses some of the preemption issues that may arise when non-federal entities attempt to regulate UAS use.

Several overarching conclusions result from the analysis presented in this Article. First, a careful examination of Supreme Court privacy jurisprudence suggests that the Constitution will provide a much stronger measure of protection against government UAS privacy abuses than is widely appreciated. The Fourth Amendment has served us well since its ratification in 1791, and there is no reason to suspect it will be unable to do so in a world where unmanned aircraft are widely used. In addition, there are substantial statutory and common law protections that will limit the ability of non-government entities to violate privacy using unmanned aircraft.

This does not mean that there is no need for additional statutory UAS privacy protections. However, when drafting new laws it is critical to adopt a balanced approach that recognizes the inherent difficulty of predicting the future of any rapidly changing technology. In the early days of the Internet and mobile phones, it would have been nearly impossible to accurately foresee all of the uses—both positive and otherwise—to which these technologies have been applied. It is similarly difficult today to predict exactly how UAS will be used—or even what they will look like—in the coming decades. Although unmanned aircraft pose real and increasingly well recognized privacy concerns, they also offer real and much less widely appreciated benefits. A dialogue conducted with full awareness of this balance will be much more likely to lead to positive policy outcomes.

I. UNMANNED AIRCRAFT SYSTEMS TECHNOLOGY

In addressing UAS privacy, it is important to start with an understanding of the technology, including both the historical context and the range of platforms that exist today. Privacy approaches designed to address only the concerns raised by the larger unmanned aircraft that have dominated much of the current press coverage may be inadequate or inappropriate for unmanned aircraft weighing only a few pounds. And, as is clear from the history of unmanned aircraft, although near-

term predictions regarding emerging aviation technology are feasible, it can be exceedingly difficult to look more than a few years into the future.

A. Historical Context: The Nineteenth and Twentieth Centuries

Unmanned flight has a long history. In fact, early research in unmanned aviation laid some of the critical groundwork that was later used by pioneers in manned aviation,[8] including the Wright Brothers, who achieved sustained manned airplane flight in 1903.[9] As early as the 1830s, William Samuel Henson was exploring the fundamentals of airframe design,[10] and in 1848 John Stringfellow successfully carried out an indoor flight of a steam-powered unmanned airplane with a wingspan of ten feet.[11] In the 1870s Alphonse Penaud demonstrated the use of twisted rubber strands as an energy source for "model"-sized airplanes and helicopters.[12] In 1896, Samuel Pierpont Langley, then Secretary of the Smithsonian Institution, flew an unmanned twin-propeller, steam-engine-powered aircraft with a wingspan of slightly under fourteen feet.[13] The aircraft, called Aerodrome Number 5, was catapult launched from a houseboat on the Potomac River and made two test flights, in each case travelling several thousand feet before landing in the river.[14]

The Sperry Aerial Torpedo, developed during World War I and demonstrated in 1918, was a bomb-equipped biplane that used an on-board timer to shut off the engine and, in theory (it was never actually used in combat), send it diving onto a tar-

---

8. Bill Hannan, *History in Models, Models in History*, MODEL AVIATION, Dec. 1986, at 78, 79–81.

9. *Milestones of Flight: 1903 Wright Flyer*, SMITHSONIAN NAT'L AIR AND SPACE MUSEUM, http://airandspace.si.edu/exhibitions/gal100/wright1903.html (last visited Jan. 28, 2013).

10. LOUIS H. HERTZ, THE COMPLETE BOOK OF MODEL AIRCRAFT SPACECRAFT AND ROCKETS 178 (1967).

11. *Id.* at 185. A two-pound steam-powered helicopter was flown even earlier, by W.D. Phillips in 1842. *Id.* at 178.

12. Hannan, *supra* note 8, at 79–81.

13. *Langley Aerodrome Number 5*, SMITHSONIAN NAT'L AIR AND SPACE MUSEUM, http://airandspace.si.edu/collections/artifact.cfm?id=A19050001000 (last visited Jan. 28, 2013).

14. *Id.*

get.[15] This was a very early example of "autonomous" flight, in which a UAS is controlled from within the aircraft, without intervention from a human on the ground.

The first unmanned airplane to be successfully flown by radio remote control was a modified N9 Navy seaplane that remained aloft for about twelve minutes during a September 1924 test, sometimes at a distance of several miles from the transmitter held by the pilot on the ground.[16] By the late 1930s, radio-controlled unmanned aircraft had started to gain significant attention in the hobbyist community[17] and in the military. During the ten-year period starting in 1934, the British military purchased hundreds of radio-controlled unmanned "Queen Bee" biplanes to use for target practice;[18] in fact, the term "drone" may have originally arisen to describe the unmanned aircraft used for this purpose.[19]

In the United States, the Radioplane Company was founded in the late 1930s[20] and during World War II built over 15,000 "drones" for the U.S. military to use in training antiaircraft gunners.[21] Radioplane was acquired by Northrop in 1952,[22] and continued to supply the U.S. military with unmanned aerial vehicles including, in the 1950s, models equipped with an on-board film-based camera.[23] Other countries with unmanned aircraft programs in the years during or shortly following World War II included Russia, France, Italy, Germany, and Japan.[24]

In the 1960s, military reconnaissance use of unmanned aircraft became increasingly common. Ryan Aeronautical Company,

---

15. *Curtiss / Sperry Aerial Torpedo*, CRADLE OF AVIATION MUSEUM, http://www.cradleofaviation.org/exhibits/ww1/sperry_torpedo/index.html (last visited Jan. 28, 2013).

16. Walt Good, *History of RC Flying*, MODEL AVIATION, Mar. 1986, at 56, 126.

17. Walt Good, *History of RC Flying, Part 2*, MODEL AVIATION Apr. 1986, at 58, 148; Walt Good, *History of RC Flying, Part 3*, MODEL AVIATION, May 1986, at 76, 76–81.

18. STEVEN J. ZALOGAUNMANNED AERIAL VEHICLES: ROBOTIC AIR WARFARE 1917–2007, at 7 (2008).

19. LAURENCE R. "NOISE" NEWCOME, UNMANNED AVIATION: A BRIEF HISTORY OF UNMANNED AERIAL VEHICLES 4 (2004).

20. *Id.* at 57.

21. ZALOGA, *supra* note 18, at 7.

22. *Id.*

23. *Id.* at 10.

24. NEWCOME, *supra* note 19, at 49–56.

which won a contract with the U.S. Air Force in 1948,[25] was a major provider of U.S. military UAS for much of the 1950s and 1960s. Versions of the Ryan Firebee flew thousands of reconnaissance and electronic warfare missions over Vietnam.[26]

The 1970s and 1980s saw continued development of military UAS technology, with the United States, Russia, Canada, Israel, and Europe all possessing active programs.[27] In the conflict with Lebanon in 1982, Israel used a relatively small UAS called the Mastiff to provide reconnaissance imagery,[28] and during the 1991 Gulf War, the U.S. military flew over 500 missions using the Pioneer UAS.[29] The Gnat-750, a precursor to the Predator, was first flown in 1989 and was employed in the mid-1990s to acquire imagery during the conflict in the former Yugoslavia.[30]

B. Unmanned Aircraft Systems Today

Since 2000, worldwide UAS use for both military and civilian applications has increased dramatically. One key factor contributing to this growth is the continuing advance of computing, imaging, and communications technologies. Computational power and storage that would have filled multiple rooms in the 1960s can now easily fit within a single chip. In the context of UAS, this has made it possible to equip even very small platforms with sophisticated on-board computational systems for tasks such as navigation and image processing. The advent of high-resolution, low-cost digital imaging systems, when combined with high-bandwidth communications links, enables high-resolution images and video acquired by an unmanned aircraft to be transmitted in real time to an observer fifty feet—or 5000 miles—away. Thanks to continuing innovations in airframe design and flight control algorithms, the cameras that can be mounted on UAS are becoming smaller and more agile.

---

25. ANTHONY FINN & STEVE SCHEDING, DEVELOPMENTS AND CHALLENGES FOR AUTONOMOUS UNMANNED VEHICLES: A COMPENDIUM 15 (2010).

26. JASJIT SINGH, AIR POWER IN MODERN WARFARE 198 (1988).

27. ZALOGA, *supra* note 18, at 16–24.

28. BENJAMIN S. LAMBETH, MOSCOW'S LESSONS FROM THE 1982 LEBANON AIR WAR 7 (1982), *available at* http://www.rand.org/pubs/reports/2007/R3000.pdf.

29. ZALOGA, *supra* note 18, at 26–28.

30. *Id.* at 29–33.

The American global positioning system (GPS),[31] which began development in 1973 and was completed in 1995,[32] has also helped to spur UAS growth. GPS makes it possible for UAS to determine their precise location using on-board systems, and therefore to perform missions involving much more complex navigational tasks than could be attempted in the pre-GPS era.[33]

Today, unmanned aircraft come in an incredible variety of shapes and sizes. Some, such as the Global Hawk used by the U.S. military, are as large and nearly as fast as business jets.[34] Others are small enough to fit in a backpack or even the palm of a hand. The video-capable Nano Hummingbird, developed by California-based AeroVironment, weighs only two-thirds of an ounce.[35] The solar-powered QinetiQ Zephyr, which weighs only slightly over 110 pounds despite having a wingspan of about 74 feet, stayed aloft for over two continuous weeks in Arizona during the summer of 2010.[36]

UAS can be controlled during flight in a variety of ways. A pilot on the ground who maintains visual contact with a UAS can fly it using a handheld or computer-based radio remote control interface. Alternatively, or in addition, in a "first-person-view" (FPV) system, a UAS-mounted camera transmits a real-time "cockpit" view to a pilot on the ground who flies

---

31. The United States developed the GPS system and, in 1983, made it available for civilian applications. MICHAEL RUSSELL RIP & JAMES M. HASIK, THE PRECISE REVOLUTION: GPS AND THE FUTURE OF AERIAL WARFARE 9–10 (2002). Russia, the European Union, China, and India have also developed or are developing comparable satellite-based positioning systems. *See* UNITED NATIONS OFFICE FOR OUTER SPACE AFFAIRS, CURRENT AND PLANNED GLOBAL AND REGIONAL NAVIGATION SATELLITE SYSTEMS AND SATELLITE-BASED AUGMENTATIONS SYSTEMS, at v (2010), *available at* http://www.oosa.unvienna.org/pdf/publications/icg_ebook.pdf.

32. Randy James, *GPS*, TIME, May 26, 2009, http://www.time.com/time/magazine/article/0,9171,1901500,00.html.

33. *See, e.g.*, Rip & Hasik, *supra* note 31, at 191–275 (discussing the role of GPS in modern warfare).

34. *RQ-4 Global Hawk Factsheet*, THE OFFICIAL WEB SITE OF THE U.S. AIR FORCE, http://www.af.mil/information/factsheets/factsheet.asp?id=13225 (last visited Jan. 28, 2013).

35. Press Release, AeroVironment Inc., AeroVironment Develops World's First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA, Feb. 17, 2011, *available at* http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird.

36. Andrew Chuter, *Solar UAV Lands After Record 2 Weeks Aloft*, DEFENSENEWS, July 23, 2010, http://www.defensenews.com/article/20100723/DEFSECT01/7230304/Solar-UAV-Lands-After-Record-2-Weeks-Aloft. The weight and length are reported in this article at 50 kilograms and 22.5 meters, respectively. *Id.*

the aircraft as if he or she were physically on-board. If the radio link between the UAS and the pilot is sufficiently strong, the UAS can be flown beyond the visual line of sight.

Autonomous flight using information from an on-board GPS receiver to perform navigation without any human intervention can also be used. Many UAS have the capability to operate in multiple modes—for example, navigating semi-autonomously to a destination based on a set of GPS waypoints input by a pilot, who then takes over active control using an FPV system. Of course, what is possible technologically and what is permitted by regulations are two very different things. At present, with very limited exceptions,[37] the Federal Aviation Administration (FAA) does not permit UAS flights in which the operator on the ground is unable to maintain continuous visual contact with the aircraft.

The UAS industry today is large, global, and rapidly growing. According to the Association for Unmanned Vehicle Systems International (AUVSI), the largest international association for unmanned systems, there are now over 400 active manufacturers of UAS globally, including 150 in the United States.[38] Other countries with significant UAS development include Australia, Brazil, Canada, China, France, Germany, India, Iran, Israel, Japan, Pakistan, Turkey, Russia, and the United Kingdom.[39] The Teal Group, an aerospace and defense consultancy based in Virginia, predicts that global annual UAS spending will rise from an estimated $6.6 billion in 2012 to over $11 billion over the next decade, corresponding to a total ten-year expenditure of nearly $90 billion.[40]

Even as overall spending is increasing, per-unit costs for the smaller platforms are dropping. Large military surveillance

---

37. The FAA Modernization and Reform Act of 2012, discussed later in this Article, includes a provision (Section 332(d)) that will allow beyond-line-of-sight operation in the Arctic (northern Alaska). *See id.* at 11–15.

38. E-Mail from Melanie Hinton, Senior Commc'ns Manager, AUVSI, to author (Aug. 15, 2012, 12:44 PDT) (on file with author).

39. U.S. Gov't Accountability Office, GAO-12-536, Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports 10–16 (2012).

40. Press Release, Teal Group Corp., Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012 UAV Market Profile and Forecast (Apr. 11, 2012), *available 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.

platforms such as the Global Hawk can cost many tens of millions of dollars or more to purchase[41] and require large teams of highly trained people using specialized equipment to fly.[42] However, there are increasing numbers of highly capable commercially available small UAS that can be purchased for under $1000. It is only a matter of time—and probably not much time—before GPS and video-equipped UAS drop below $100, and then below $10.

UAS can be used in law enforcement, search and rescue, surveying, scientific research, and many other civilian applications. Although many people equate the prospect of law enforcement use of UAS with surveillance, in practice this may be the exception rather than the rule. In this respect, the experience of the Mesa County, Colorado, Sheriff's Office is instructive. Mesa County has one of the only current FAA Certificates of Authorization for operational (as opposed to training) use of UAS.[43] The Mesa County Sheriff's Office has (as of February 2013) flown approximately 40 missions since 2011, and has never used them to perform surveillance.[44] Instead, typical operations have been for obtaining after-the-fact crime scene images, search and rescue, and providing imagery for structure fire suppression and arson investigations. Ben Miller, the Unmanned Aircraft Program Manager in Mesa County, puts the per-hour operating cost of Mesa County's UAS at $25;[45] a manned helicopter, by contrast, costs hundreds of dollars per hour to operate. The dramatically lower operating cost for unmanned aircraft provides a powerful economic incentive for their adoption. In addition, they can be used in circumstances where a manned helicopter would have been too dangerous or disruptive.

---

41. A U.S Government Accountability Office report put the "unit cost" of a Global Hawk at $176 million as of July 2010. MICHAEL J. SULLIVAN, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-233SP, DEFENSE ACQUISITIONS: ASSESSMENTS OF SELECTED WEAPON PROGRAMS 69 (2011), *available at* http://www.gao.gov/assets/320/317081.pdf.

42. *See, e.g., RQ-4 Global Hawk*, U.S. AIR FORCE, http://www.af.mil/information/factsheets/factsheet.asp?id=13225 (last visited Jan. 28, 2013).

43. E-Mail from Benjamin Miller, Unmanned Aircraft Program Manager, Mesa Cnty. Sheriffs Office, to author (Aug. 13, 2012, 10:45 PDT) (on file with author).

44. E-Mail from Benjamin Miller, Unmanned Aircraft Program Manager, Mesa Cnty. Sheriffs Office, to author (Feb. 7, 2013, 7:02 PST) (on file with author).

45. E-Mail from Benjamin Miller, Unmanned Aircraft Program Manager, Mesa Cnty. Sheriffs Office, to author (Aug 15, 2012, 13:19 PDT) (on file with author).

In Australia, where certain commercial operations using small unmanned aircraft have been permitted for over ten years,[46] applications have included mining surveys and transportation of equipment to drilling rigs.[47] In Japan, agricultural spraying is often performed using small unmanned helicopters.[48] In the United States, NASA researchers have used UAS for studying Hawaiian volcanoes.[49] UAS are also ideal platforms for identifying wildfire hotspots without putting a human pilot at risk.[50]

II. REGULATORY FRAMEWORK

A. The Federal Aviation Administration

When considering the regulatory framework applicable to UAS in the United States, it is helpful to start by briefly addressing how aircraft operations in general are regulated. The FAA, which was established in 1958 and has been part of the

---

46. *See* Duncan Jefferies, *Drone journalism set for takeoff – once they're permitted to use our airspace*, THE GUARDIAN MEDIA NETWORK BLOG (Oct. 29, 2012, 7:09 AM), http://www.guardian.co.uk/media-network/media-network-blog/2012/oct/29/drone-journalism-take-off (noting that commercial drones have been licensed in Australia since 2002); *see also* Australia Civil Aviation Safety Authority Advisory Circular 101-1(0), *Unmanned Aircraft and Rockets: Unmanned Aerial Vehicle (UAV) Operations, Design Specification, Maintenance and Training of Human Resources* (July 2002), *available at* http://www.casa.gov.au/wcmswr/_assets/main/rules/1998casr/101/101c01.pdf. The Advisory Circular states "Provided that a small UAV is operated not above 400ft AGL [above ground level] and remains clear of designated airspace, aerodromes and populous areas, there are no restrictions imposed upon the operation of a small UAV." *Id.* § 7.1.1. The Australia Civil Aviation Safety Authority defines "small" UAS as those weighing under 150 kilograms. *See* Gary Carr, *Unmanned Aircraft CASA Regulations* 2, Australian Gov't Civil Aviation Safety Auth., *available at* http://www.uatar.com/CASA%20Presentation%20-%20Unmanned%20Aircraft%20CASA%20Regulations.pdf.

47. Ry Crozier, *Australian miners send drones to work*, ITNEWS, May 28, 2012, http://www.itnews.com.au/News/302240,australian-miners-send-drones-to-work.aspx.

48. REG AUSTIN, UNMANNED AIRCRAFT SYSTEMS: UAVS DESIGN, DEVELOPMENT AND DEPLOYMENT 273–74 (2010).

49. Mark Brown, *Nasa sends UAV back to explore explosive Hawaiian volcano*, WIRED.CO.UK, Apr. 5, 2011, http://www.wired.co.uk/news/archive/2011-04/5/nasa-sends-out-volcano-spying-drone.

50. Brian Bennett, *Drones tested as tools for police and firefighters*, L.A. TIMES, Aug. 5, 2012, http://articles.latimes.com/2012/aug/05/nation/la-na-drones-testing-20120805.

Department of Transportation since the 1960s,[51] oversees nearly all[52] aircraft operations in the United States.[53] This is a complex task in a national airspace that has an "average of more than 100,000 aviation operations per day, including air carrier, air taxi, general aviation, and military aircraft."[54]

Like other administrative agencies of the United States government, the FAA makes and enforces rules to implement and interpret laws passed by Congress.[55] New rules,[56] such as those to be developed by the FAA to enable the integration of UAS into the airspace, are formulated through a rulemaking process that includes an internal drafting and review stage, publication of a draft rule in the Federal Register, a period of public comment, revisions based on the comments, and publication of a final rule.[57]

---

51. *A Brief History of the FAA*, FED. AVIATION ADMIN., http://www.faa.gov/about/history/brief%5Fhistory/http://www.faa.gov/about/history/brief_history/ (last visited Nov. 10, 2012) [hereinafter *Brief History*].

52. There are a few exceptions. For example, the FAA does not have any responsibility to ensure the separation of military aircraft operating within "MARSA" airspace. MARSA is an acronym for "Military Assumes Responsibility for Separation of Aircraft." FED. AVIATION ADMIN., AIR TRAFFIC ORG. POLICY ¶ 2-1-11 (2012), *available at* http://www.faa.gov/air_traffic/publications/atpubs/atc/atc0201.html. In addition, the FAA does not oversee model aircraft operated in accordance with FAA Advisory Circular 91-57 or with Section 336 of the FAA Modernization and Reform Act of 2012, which creates a special rule for model aircraft. *See* FED. AVIATION ADMIN., ADVISORY CIRCULAR 91-57, MODEL AIRCRAFT OPERATING STANDARDS (1981) [hereinafter ADVISORY CIRCULAR 91-57], *available at* http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf; FAA Modernization and Reform Act of 2012 (FMRA), Pub. L. No. 112-95, § 336, 126 Stat. 11, 77 (2012).

53. Brief History, supra note 51.

54. *Fact Sheet: Unmanned Aircraft Systems (UAS)*, FED. AVIATION ADMIN., http://www.faa.gov/about/initiatives/uas/media/uas_fact_sheet.pdf (last visited Jan. 28, 2013) [hereinafter *Fact Sheet*].

55. Formally, a "rule" is "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy. . . ." Administrative Procedure Act § 1, 5 U.S.C. § 551(4) (2012).

56. FAA "rules" are also called "regulations." *See, e.g.*, 49 U.S.C. § 40103 (directing that the Administrator of the FAA promulgate "regulations" governing the flight of aircraft).

57. There are actually various forms of rulemaking in accordance with the Administrative Procedure Act, which was enacted in 1946. The steps described in the text (and provided in 5 U.S.C. § 553) occur in association with what is referred to as informal rulemaking, which is by far the most common form. There is also a formal rulemaking process under 5 U.S.C. §§ 556–557 that includes a hearing and

FAA regulations[58] classify aircraft, without regard to whether they are manned, as either "public"[59] or "civil."[60] Public aircraft are those operated by local, state, and federal public entities, including law enforcement agencies.[61] Civil aircraft, typically, are operated by private companies, individuals, and other non-government entities. The public-civil distinction is extremely important both generally and with respect to UAS.

B. The FAA and Unmanned Aircraft Systems

On February 14, 2012, President Obama signed the FAA Modernization and Reform Act of 2012 (FMRA)[62] into law. FMRA provides, among other things, a set of overlapping deadlines for the integration of UAS into the national airspace over the next three years.[63] Although UAS integration has been on the proverbial radar screen of the FAA for a number of years, FMRA represents the first significant congressional legislation addressing the domestic use of UAS.

---

a number of other steps. RAYMOND C. SPECIALE, FUNDAMENTALS OF AVIATION LAW 124–25 (2006).

58. FAA regulations are provided in the Code of Federal Regulations (CFR), Title 14 ("Aeronautics and Space"), Volumes 1–3, which comprise parts 1–199 (not all of the numbers in this range are currently used). "General Operating and Flight Rules" for aircraft are found in Volume 2, Subchapter F ("Air Traffic and General Operating Rules"), Part 91, denoted 14 C.F.R. § 91 and sometimes referred to as FAR Part 91. FAR is an acronym for "Federal Aviation Regulations." "General Definitions" are in 14 C.F.R. § 1.1. An unofficial version of the CFR is provided through the Electronic Code of Federal Regulations (e-CFR) by the government at http://ecfr.gov.

59. Section 331(4) of the FAA Modernization and Reform Act provides that "[t]he term 'public unmanned aircraft system' means an unmanned aircraft system that meets the qualifications and conditions required for operation of a public aircraft . . . ." FAA Modernization and Reform Act of 2012 (FMRA), Pub. L. No. 112-95, § 331, 126 Stat. 11, 72 (2012). The term "public aircraft" is defined in 49 U.S.C.A. § 40102(a)(41) (2012), as well as in 14 C.F.R. § 1.1 (2012).

60. *See* 49 U.S.C. § 40102(a)(16).

61. *See* § 40102(a)(41). Whether an aircraft has "public aircraft status" depends, in part, on how it is being used. An aircraft that is owned by a government entity but engaged in an operation that replicates a service that could be obtained from a commercial air carrier does not have public aircraft status during that operation. As used in this Article, "public aircraft" and "government aircraft" refer to aircraft that satisfy the statutory qualifications for public aircraft status under § 40125.

62. Pub. L. No. 112-95, 126 Stat. 11 (2012).

63. *Id.* §§ 331–336, 126 Stat. at 72–78.

Recognizing that UAS raise unique issues that "may differ substantially from manned aircraft operations and systems,"[64] the FAA created a new Unmanned Aircraft Program Office in early 2006.[65] In accordance with policies established well before the enactment of FMRA, operators of UAS engaged in public aircraft operations are required to obtain a Certificate of Authorization (COA).[66] Civil (i.e. private) UAS operators need a "special airworthiness certificate."[67] Use of UAS for commercial purposes is currently prohibited,[68] though that is expected to change by 2014.

According to data released in early 2012 in response to a Freedom of Information Act lawsuit filed by the Electronic Frontier Foundation, the FAA had issued "about 700–750 authorizations since the program began in 2006," of which approximately 300 remained active as of April 2012.[69] Public entities that have been issued COAs include the U.S. Air Force,

---

64. James Sizemore & Richard Posey, Fed. Aviation Admin., Unmanned Aircraft Systems (UAS) Certification Status 2 (2006), *available at* http://www.faa.gov/about/initiatives/uas/reg/media/uas_policyupdate.pdf.

65. *Id.* at 1.

66. *See* DEP'T. OF TRANSP., UNMANNED AIRCRAFT OPERATIONS IN THE NATIONAL AIRSPACE SYSTEM, DOCKET NO. FAA-2006-25714 (2007), *available at* http://www.faa.gov/about/initiatives/uas/reg/media/frnotice_uas.pdf. In addition to "Certificate of Authorization," COA is sometimes written in expanded form as "Certificate of Waiver or Authorization" or "Certificate of Authorization or Waiver." *See id.* An exception to the COA requirement is MARSA airspace. *See supra* note 52.

67. *See* 14 C.F.R. § 21.175 (2012). Although model aircraft are obviously unmanned, provided that they are flown for hobby or recreational use, they are not treated as "civil UAS" by the FAA. *See* ADVISORY CIRCULAR 91-57, *supra* note 52; FMRA § 336, 126 Stat. at 77.

68. Even though this prohibition is not explicit with respect to UAS, it is implicit in the list, provided in 14 C.F.R. § 21.191, of purposes for which experimental certificates can be issued. To date, special airworthiness certificates have been issued only in the experimental category. *Fact Sheet, supra* note 54, at 146 ("An SAC-EC is the only certification means available to civil operators for UAS and optionally-piloted aircraft (OPA)."). "SAC" is an acronym for special airworthiness certificate. The list in § 21.191 includes purposes such as "[r]esearch and development," "[a]ir racing," and "[c]rew training," but not commercial use. In addition, 14 C.F.R. § 91.319, which describes operating limitations for aircraft having experimental certificates, provides, among other things, that "[n]o person may operate an aircraft that has an experimental certificate—(1) For other than the purpose for which the certificate was issued; or (2) Carrying persons or property for compensation or hire."

69. Jennifer Lynch, *FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered.

U.S. Army, the Defense Advanced Research Projects Agency (DARPA), FBI, NASA, some county and municipal law enforcement agencies, and various public universities.[70] The list of companies that have been issued special airworthiness certificates includes Raytheon, Honeywell, General Atomics, and other defense companies.[71]

COAs specify where and under what circumstances a UAS can be used. For example, a COA might require that the UAS only be flown during daylight hours, and only within the visual line of sight of the operator.[72] In the case of a UAS operated by a law enforcement agency, the COA might specify that flights must be performed only for training, as opposed to operational, purposes. In early 2008, the FAA began the process of developing recommendations for regulating "small" UAS (those weighing under fifty-five pounds).[73] Thus, by the time FMRA was signed into law in February 2012, the FAA had already been actively planning for UAS integration for several years.

FMRA sets a goal of integrating UAS into the national airspace system by late 2015.[74] Under the new law, public UAS operators have had access to expedited COAs since May 14, 2012.[75] UAS under these authorizations must weigh no more than twenty-five pounds[76] and be operated within the line of sight of the op-

---

70. *FAA List of Certificates of Authorizations (COAs)*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/document/faa-list-certificates-authorizations-coas (last visited Jan. 28, 2013).

71. *FAA List of Special Airworthiness Certificates – Experimental Category (SACs)*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/document/faa-list-special-airworthiness-certificates-experimental-categorysacs (last visited Jan. 28, 2013).

72. *Fact Sheet*, *supra* note 54, at 2.

73. In April 2008, the FAA created the Small Unmanned Aircraft System Aviation Rulemaking Committee. *See* FED. AVIATION ADMIN., ORDER 1110.150, SMALL UNMANNED AIRCRAFT SYSTEM AVIATION RULEMAKING COMMITTEE (2008), http://www.faa.gov/documentLibrary/media/Order/1110.150.pdf. This committee is often referred to using the acronym sUAS ARC, and has members from both government and industry. The sUAS ARC issued a set of recommendations for sUAS regulatory development in April 2009. *See* FED. AVIATION ADMIN., SMALL UNMANNED AIRCRAFT SYST. AVIATION RULEMAKING COMM., COMPREHENSIVE SET OF RECOMMENDATIONS FOR SUAS REGULATORY DEVELOPMENT (2009), *available* at http://www.modelaircraft.org/faa/recommendations.pdf.

74. FMRA, Pub. L. No. 112–95, § 332(a)(3), 126 Stat. 11, 73 (2012).

75. *See id.* § 334(c), 126 Stat. at 76.

76. *FAA Makes Progress with UAS Integration*, FED. AVIATION ADMIN., http://www.faa.gov/news/updates/?newsId=68004 (last visited Jan. 28, 2012). Interestingly, with respect to weight, the FAA went further than was required by

erator, less than 400 feet above the ground, and during daylight conditions.[77] By December 31, 2015, the FAA is required to "develop and implement operational and certification requirements for the operation of public unmanned aircraft systems in the national airspace system by September 30, 2015."[78]

For civil UAS, FMRA mandates the development of a "comprehensive plan" that will "provide for the safe integration of civil unmanned aircraft systems into the national airspace."[79] Additionally, regulations for the operation of small civil UAS (including allowing their use for commercial purposes) are due by August 2014.[80]

The FAA is in somewhat of a unique position with respect to deadlines laid out in legislation such as FMRA. FMRA requires that the FAA "provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, but not later than September 30, 2015."[81] This language contains no explicit provision for what happens if, in the FAA's view, "as soon as practicable" is later than that date. However, Congress is unlikely to hold the FAA to a deadline that might risk jeopardizing airspace safety.

C. *The Impact of Safety Regulations on Privacy*

Though privacy and airspace safety are distinct UAS issues, they are in some respects closely intertwined. By placing limitations on where and how unmanned aircraft can be operated, airspace safety regulations can impact privacy.

For example, under the FAA regulations that prescribe "flight rules governing the operation of [both manned and un-

---

FMRA, which provided that the authorizations must "allow a government public safety agency to operate unmanned aircraft weighing 4.4 pounds or less." FMRA § 334(c)(2)(C), 126 Stat. at 77.

77. These requirements are among those provided in FMRA § 334(c)(2)(C). Additional requirements in this Section restrict operation to Class G (uncontrolled) airspace more than five miles from airports and other locations with aviation activities. *See id.*

78. *Id.* § 334(b), 126 Stat. at 76.

79. *Id.* § 332(a)(1).

80. *Id.* § 332(b)(1).

81. *Id.* § 332(a)(3).

manned] aircraft within the United States,"[82] it is illegal to operate an aircraft "in a careless or reckless manner so as to endanger the life or property of another."[83] Aircraft must also be operated at a sufficiently high altitude to allow "an emergency landing without undue hazard to persons or property on the surface" in the event of an engine failure.[84] Compliance with these rules, which apply to both manned and unmanned aircraft,[85] could be called into question, for example, in the monitoring of a peaceful protest if a UAS is flown (either by law enforcement or by a protester) at very low altitudes directly above a crowd of people.[86]

The tie between safety and privacy is tightest with respect to rules requiring the operator of a UAS to be able to see the aircraft at all times. Public UAS operated in association with the expedited authorizations in Section 334(c)(2)(C) of FMRA have a "line of sight" requirement.[87] The rules for civil small UAS due for implementation in August 2014 likely will also have this constraint. From the FAA's standpoint, any such requirement would be solely motivated by safety concerns related to the need to "sense and avoid" other aircraft and to problems that might arise if a UAS beyond the line of sight loses communication with its operator.[88] But there are privacy consequences as well.

It is easy for an operator standing on the street in front of a house to fly a UAS high enough to obtain overhead images of a fenced-in backyard while maintaining visual contact with the

---

82. Subpart B of part 91 applies to "the operation of aircraft within the United States and within 12 nautical miles from the coast of the United States." 14 C.F.R. § 91.101 (2012).

83. 14 C.F.R. § 91.13(a).

84. 14 C.F.R. § 91.119(a).

85. *See* 14 C.F.R. § 91.1(a) (stating that part 91 "govern[s] the operation of aircraft . . . within the United States.").

86. *See* 14 C.F.R. § 91.13(a).

87. FMRA § 334(c)(2)(c).

88. *See Fact Sheet*, *supra* note 54, at 2. Not everyone in the unmanned aviation community is in agreement regarding the safety value of a line of sight requirement. Opponents of such a requirement could argue, among other things, that a UAS beyond the visual line of sight that loses communication with an operator can be programmed to land itself safely. Opponents could also argue that even if a UAS is within visual line of sight, if the ability of the operator to communicate with it is lost, being able to see it does little to mitigate any resulting risks. Nonetheless, this is an area in which regulators are likely to act very conservatively.

aircraft. It is far harder, by contrast, to maintain visual line of sight while lowering the UAS into the yard to obtain eye-level images through the back windows of the house. Thus, the questions of if, when, and under what circumstances non-visual line of sight operation will be permitted will have an impact on privacy.[89]

Even assuming that FAA regulations adopted in the next several years continue to require visual line of sight operation, in the longer term this requirement is likely to be relaxed for some specific classes of UAS operations. Some of the most promising applications of UAS, by their very nature, require non-visual line of sight operation. For example, UAS have enormous potential for search and rescue in large part because they can enable an operator to quickly and safely examine many square miles of potentially inhospitable terrain. Surveying of pipelines, long-distance electric transmission lines, and other extended structures can also entail large separations between an operator and a UAS. As "sense and avoid" technologies become more mature, these sorts of non-line of sight operations may eventually be permitted. This will expand ways in which a UAS flown in compliance with FAA regulations might be used to violate privacy.

III. GOVERNMENT UNMANNED AIRCRAFT AND THE FOURTH AMENDMENT

The Fourth Amendment is central to the privacy issues with respect to government UAS operation. Although the Supreme Court has never explicitly considered the question of UAS privacy, there is a long list of relevant precedents.[90] Among them

89. The term "line of sight" is more complex than it first appears. Some people in the UAS community use "line of sight" to refer to operation in which a radio signal can be transmitted directly from an operator to a UAS, without being relayed through a satellite, other aircraft, or ground-based communications network (sometimes also called "electronic line of sight"). This does not ensure that the operator can necessarily see the UAS, as radio signals can easily pass through trees and other objects, sometimes traveling for miles. The term "*visual* line of sight," by contrast, is unambiguous: The operator must be able to see, with his or her eyes, the UAS.

90. In addition to the cases discussed at greater length in Part III of this Article, see, e.g., City of Indianapolis v. Edmond, 531 U.S. 32 (2000), Minnesota v. Carter, 525 U.S. 83 (1998), United States v Karo, 468 U.S. 705 (1984), Oliver v. United States, 466 U.S. 170 (1984), United States v. Knotts, 460 U.S. 276 (1983), Steagald v.

are several cases from the 1980s that specifically considered aerial observations and the Fourth Amendment. The 2001 *Kyllo v. United States*[91] and 2012 *United States v. Jones*[92] decisions are also pertinent.

A. Dow Chemical Co. v. United States

In 1978, the Environmental Protection Agency, without Dow Chemical's consent, contracted with a commercial aerial photographer to provide images of a 2000-acre Dow Chemical manufacturing facility from altitudes of 1200, 3000, and 12,000 feet.[93] When Dow Chemical became aware of this, it filed suit in Federal District Court, which granted summary judgment, finding the aerial photography to be a search in violation of the Fourth Amendment.[94] The Sixth Circuit reversed the decision, ruling that even though the company had taken precautions, including installing a perimeter fence and alarm system[95] that provided a subjective expectation of privacy from ground-level intrusions, it did not have such an expectation with respect to aerial surveillance.[96] Thus, the Sixth Circuit concluded, the acquisition of aerial images without a warrant was not a Fourth Amendment search.[97]

In reviewing this ruling on certiorari, the Supreme Court affirmed the Sixth Circuit's decision, concluding in a 1986 ruling that the open areas in the 2000-acre industrial facility were more akin to an "open field"[98] than to the curtilage of a home,

---

United States, 451 U.S. 204 (1981), Smith v. Maryland, 442 U.S. 735 (1979), Rakas v. Illinois, 439 U.S. 128 (1978), City of Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624 (1973), Katz v. United States, 389 U.S. 347 (1967), Camara v. Mun. Court, 387 U.S. 523 (1967), Griggs v. Allegheny Cnty., 369 U.S. 84 (1962), Silverman et al. v. United States, 365 U.S. 505 (1961), Johnson v. United States, 333 U. S. 10 (1948), United States v. Causby, 328 U.S. 256 (1946), Hester v. United States, 265 U.S. 57 (1924), and Boyd v. United States, 116 U.S. 616 (1886).

91. 533 U.S. 27 (2001).

92. 132 S. Ct. 945 (2012).

93. Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).

94. *Id.* at 230.

95. *Id.* at 240–41 (Powell, J., concurring in part and dissenting in part).

96. *Id.* at 230.

97. *Id.* at 229.

98. The Court wrote that "open fields do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from governmental interference or surveillance" and that "an individual may not legitimately demand privacy for activities out of doors in fields, except in the area immedi-

and, as a result, were "open to the view and observation of persons in aircraft lawfully in the public airspace immediately above or sufficiently near the area for the reach of cameras."[99] The Court also noted the role of technology diffusion as a factor, writing that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[100] However, the Court observed, "[a]ny person with an airplane and an aerial camera could readily duplicate"[101] the photographs at issue. "[T]he taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[102]

B. California v. Ciraolo

Ciraolo[103] was decided in 1986, on the same day as *Dow Chemical*. On September 2, 1982, police in Santa Clara, California, received a tip regarding backyard marijuana cultivation.[104] After finding the yard surrounded by high fencing obscuring the view from the street, they obtained a small airplane and flew over the residence at 1000 feet.[105] The officers on the airplane observed and photographed what they concluded to be marijuana plants growing in the backyard.[106] This evidence was used to obtain a search warrant to seize the plants.[107]

The Supreme Court granted certiorari after the California Court of Appeal ruled that the warrantless aerial observations violated the Fourth Amendment.[108] In May 1986, the Supreme Court issued a five-to-four decision reversing the lower court.[109] Writing for the majority, Chief Justice Burger framed

---

ately surrounding the home." *Id.* at 235–36 (alteration in original) (quoting Oliver v. United States, 466 U.S. 170, 178–79 (1984)) (internal quotation marks omitted).

99. *Id.* at 239.

100. *Id.* at 238.

101. *Id.* at 231.

102. *Id.* at 239.

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

104. *Id.* at 209.

105. *Id.*

106. *Id.*

107. *Id.*

108. People v. Ciraolo, 161 Cal. App. 3d 1081, 1090 (Ct. App. 1984).

109. *Ciraolo*, 476 U.S. at 215.

the analysis in terms of the "reasonable expectation of privacy"[110] articulated in Justice Harlan's concurrence in *Katz*.[111] For an expectation of privacy to be "reasonable" under *Katz*, two separate criteria must be satisfied. First, the person must "have exhibited an actual (subjective) expectation of privacy."[112] Second, the expectation must "be one that society is prepared to recognize as 'reasonable.'"[113]

With respect to the first criterion, the *Ciraolo* Court wrote that although the presence of fences clearly conveyed a "desire to maintain privacy," and indeed successfully did so with respect to "normal sidewalk traffic," the marijuana plants might well have been visible from a truck or two-level bus.[114] Thus, it was unclear that the respondent had "a subjective expectation of privacy from all observations of his backyard."[115]

With respect to the second criterion, the Court did not dispute that the backyard was in the curtilage of the home,[116] but noted that police observations of curtilage are not necessarily unconstitutional. "The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[117] Moreover, "the mere fact that an individual has taken measures to restrict some views of his activities [does not] preclude an officer's observations from a public vantage

---

110. *Id.* at 211.

111. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

112. *Id.* at 361.

113. *Id.* Much turns on the interpretation of "reasonable." For example, in *Illinois v. Caballes*, the Supreme Court explained that "the expectation 'that certain facts will not come to the attention of the authorities' is not the same as an interest in 'privacy that society is prepared to consider reasonable.'" 543 U.S. 405, 408–09 (2005) (quoting United States v. Jacobsen, 466 U.S. 109, 122 (1984)). In *Caballes*, the Court also distinguished between legitimate privacy expectations with respect to lawful, as opposed to unlawful, activity: "The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car." *Id.* at 410.

114. *Ciraolo*, 476 U.S. at 211.

115. *Id.* at 211–12.

116. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 180 (1984) ("Thus, courts have extended Fourth Amendment protection to the curtilage; and they have defined the curtilage, as did the common law, by reference to the factors that determine whether an individual reasonably may expect that an area immediately adjacent to the home will remain private.").

117. *Ciraolo*, 476 U.S. at 213.

point where he has a right to be and which renders the activities clearly visible."[118] Because the observations were made from "public navigable airspace . . . in a physically nonintrusive manner," the respondent's expectation of privacy from such aerial observations was not one "that society is prepared to honor."[119] The Court concluded that "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."[120]

The dissent, delivered by Justice Powell, criticized the Court's reliance on the absence of a "physical invasion of the curtilage" in finding no constitutional violation: "Since *Katz*, we have consistently held that the presence or absence of physical trespass by police is constitutionally irrelevant to the question whether society is prepared to recognize an asserted privacy interest as reasonable."[121] The dissent also disagreed with the Court's view that conducting an overflight with the specific goal of enabling trained officers to observe a suspect's backyard raised no more constitutional questions than overflights by members of the flying public: "[T]he actual risk to privacy from commercial or pleasure aircraft is virtually nonexistent. Travelers on commercial flights, as well as private planes used for business or personal reasons, normally obtain at most a fleeting, anonymous, and nondiscriminating glimpse of the landscape and buildings over which they pass."[122] And, in an observation that would foreshadow the *Kyllo* decision fifteen years later, Justice Powell warned that "[r]apidly advancing technology now permits police to conduct surveillance in the home itself, an area where privacy interests are most cherished in our society, without any physical trespass."[123]

---

118. *Id.*

119. *Id.* at 213–14.

120. *Id.* at 215.

121. *Id.* at 223 (Powell, J., dissenting).

122. *Id.* In a footnote to this text, Justice Powell called the Court's "analogy to commercial and private overflights" "wholly without merit." *Id.* at 223 n.8.

123. *Id.* at 226.

C. Florida v. Riley

Just under three years after *Ciraolo*, the Supreme Court once again ruled on the constitutionality of aerial observations of a home's curtilage by law enforcement. Like *Ciraolo*, *Florida v. Riley*[124] arose from a tip involving marijuana cultivation behind a house, where the plants could not be seen from the street. In *Riley*, the observations were made from a helicopter at 400 feet, enabling officers to see the plants through openings in the roof and sides of a greenhouse located behind a mobile home.[125] A majority of the justices in *Riley* found these observations constitutional.

Writing for the plurality,[126] Justice White wrote that "our decision in *California v. Ciraolo* controls this case."[127] While Riley took steps that "protected against ground-level observation," "the sides and roof of his greenhouse were left partially open" and "what was growing in the greenhouse was subject to viewing from the air."[128] "Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more."[129]

Despite Justice White's statement that "[w]e would have a different case if flying at that altitude had been contrary to law or regulation,"[130] his opinion also provided an important qualifier: "This is not to say that an inspection of the curtilage of a house from an aircraft will always pass muster under the Fourth Amendment simply because the plane is within the navigable airspace specified by law."[131] Specifically, in ruling that there was no violation of the Fourth Amendment in the present case, Justice White found it of note that "no intimate

---

124. 488 U.S. 445 (1989).

125. *Id.* at 448.

126. The *Riley* decision comprised an opinion delivered by Justice White and joined by Chief Justice Rehnquist and Justices Scalia and Kennedy; an opinion from Justice O'Connor concurring in the judgment; a dissent from Justice Brennan joined by Justices Marshall and Stevens; and a separate dissent filed by Justice Blackmun. Thus, even though there was no majority opinion, a majority of the Justices found the observations constitutional.

127. *Id.* at 449 (plurality opinion) (internal citation omitted).

128. *Id.* at 450.

129. *Id.* at 451.

130. *Id.*

131. *Id.*

details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury."[132]

In her opinion concurring in the judgment, Justice O'Connor raised concerns about relying on "compliance with FAA regulations alone" as a litmus test for privacy from overhead surveillance.[133] Rather, she wrote, "consistent with *Katz*, we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not 'one that society is prepared to recognize as reasonable.'"[134] She then concluded that because there is "considerable public use of airspace at altitudes of 400 feet and above," Riley did not have a reasonable expectation of privacy from naked-eye observations from that altitude.[135] However, she wrote, "public use of altitudes lower than that—particularly public observations from helicopters circling over the curtilage of a home—may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy, despite compliance with FAA air safety regulations."[136]

Justice Brennan's dissent also took issue with the tie between FAA safety regulations and privacy: "It is a curious notion that the reach of the Fourth Amendment can be so largely defined by administrative regulations issued for purposes of flight safety."[137] He observed that the police officer's "ability to see over Riley's fence depended on his use of a very expensive and sophisticated piece of machinery to which few ordinary citizens have access."[138] The question, in Justice Brennan's view, was not whether the flights were in compliance with the FAA regulations, "but whether public observation of Riley's curtilage was so commonplace that Riley's expectation of privacy in his backyard could not be considered reasonable."[139] And while privately owned helicopters occasionally fly over populated areas

---

132. *Id.* at 452.
133. *Id.* at 453 (O'Connor, J., concurring in the judgment).
134. *Id.* at 454 (quoting Katz v. United States, 389 U.S. 347,361 (1967)).
135. *Id.* at 455.
136. *Id.*
137. *Id.* at 458 (Brennan, J., dissenting).
138. *Id.* at 460.
139. *Id.*

at 400 feet, "such flights are a rarity."[140] Justice Blackmun's dissent also cited the rarity of helicopter overflights at 400 feet and stated that for any observations below 1000 feet (the altitude of the fixed-wing aircraft in *Ciraolo*), the prosecution should have the burden of proving that a suspect whose curtilage was observed lacked a reasonable expectation of privacy.[141]

D. Kyllo v. United States

Although *Kyllo*[142] involved ground-based observations of a home, the case is nonetheless highly relevant to privacy from aerial observations; in fact, *Ciraolo* was invoked multiple times in the Court's 2001 *Kyllo* opinion. In January 1992, a government agent in a car used a thermal imaging device to measure the external temperature of the roof and outside wall of the home of Danny Lee Kyllo, who was suspected of growing marijuana.[143] The roof and wall were found to be abnormally warm, and a search warrant was issued based in part on this information.[144] Upon execution of the search warrant, marijuana plants were found and Kyllo was arrested.[145] A district court and the Ninth Circuit upheld the use of the thermal imager, in part on the grounds that it "merely indicated amorphous 'hot spots' on the roof and exterior wall and not the detailed images of private activity."[146]

The Supreme Court reversed the Ninth Circuit in a five-to-four opinion delivered by Justice Scalia.[147] The Court framed its analysis by noting that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass."[148] More recent rulings have "decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property, but the lawfulness of warrantless visual surveillance of a home has still been preserved."[149] However, with

---

140. *Id.* at 465.
141. *Id.* at 468 (Blackmun, J., dissenting).
142. Kyllo v. United States, 533 U.S. 27 (2001).
143. *Id.* at 29–30.
144. *Id.* at 30.
145. *See id.*
146. United States v. Kyllo, 190 F.3d 1041, 1047 (9th Cir. 1999).
147. *Id.* at 29.
148. *Id.* at 31.
149. *Id.* at 32 (citation omitted).

respect to searches of the interior of a home, "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."[150]

The Court expressed concern that allowing the government to freely collect any information "emanating from a house" would put people "at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[151] The Court also noted that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[152] The Court then concluded that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[153]

In dissent, Justice Stevens criticized the Court for, in his view, failing to follow established principles providing that searches inside a home are presumptively unreasonable, while searches of property "in plain view" are not.[154] Justice Stevens also wrote that "any member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces," and that "[h]eat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building."[155] Justice Stevens also criticized the Court's use of a standard that would diminish privacy protection as "intrusive equipment becomes more readily available."[156] Indeed, in the decade following *Kyllo*, thermal imagers have become less ex-

---

150. *Id.* at 34.

151. *Id.* at 35–36.

152. *Id.* at 36.

153. *Id.* at 40.

154. *Id.* at 42 (Stevens, J., dissenting) (quoting Payton v. New York, 445 U.S. 573, 586–87 (1980)).

155. *Id.* at 43–44.

156. *Id.* at 47. Justice Stevens also disputed the Court's "assumption that the thermal imager used in this case" was not in general public use, and noted in a footnote that similar imagers were available for rental through a toll-free telephone number. *Id.* at 47 & n.5.

pensive and more widely available. Writing in 2010, Orin Kerr observed that "remote infrared temperature-sensing has become quite common in a wide range of applications" and "it seems to me that there's at least a plausible case that the police can now use thermal imaging devices—or at least the simple single-point infrared devices—without a warrant."[157]

E. United States v. Jones

The most recent major Supreme Court privacy ruling is *United States v. Jones*,[158] decided in January 2012. In September 2005, agents on a joint FBI and Metropolitan (Washington D.C.) Police Department task force installed, without a valid warrant,[159] a GPS tracking device on a vehicle used by a suspect in a narcotics investigation.[160] The GPS tracker collected location data for approximately one month, and was used to place the suspect, Antoine Jones, at a house at a date and time where drug sales allegedly occurred.[161] After two trials in the United States District Court for the District of Columbia (the first ended in a mistrial), Jones and another defendant were convicted on a drug conspiracy charge.[162]

On appeal, Jones' conviction was overturned.[163] While noting that a person's reasonable expectation of privacy is highest in his or her home, the District of Columbia Circuit Court of Appeal recognized that "[a] person does not leave his privacy behind when he walks out his front door . . . . On the contrary, in *Katz* the Court clearly stated 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally

---

157. Orin Kerr, Can the Police Now Use Thermal Imaging Devices Without a Warrant? A Reexamination of Kyllo in Light of the Widespread Use of Infrared Temperature Sensors, THE VOLOKH CONSPIRACY, (Jan. 4, 2010, 12:33 PM), http://www.volokh.com/2010/01/04/can-the-police-now-use-thermal-imaging-devices-without-a-warrant-a-reexamination-of-kyllo-in-light-of-the-widespread-use-of-infrared-temperature-sensors/.

158. 132 S. Ct. 945 (2012).

159. The agents had obtained a warrant, but it was for the District of Columbia and was valid for a ten-day period. The agents installed the tracking device in Maryland on the eleventh day. *See id.* at 948.

160. *Id.*

161. *Id.* at 948–49.

162. *Id.*

163. *Id.* at 949.

protected.'"[164] In using the warrantless GPS tracker to discover "the totality and pattern of his movements," the court concluded that the government violated the Fourth Amendment.[165]

The Supreme Court granted the government's petition of certiorari.[166] The Court's January 2012 decision was unanimous in finding the government's actions unconstitutional, but the Justices widely diverged in the bases for that finding. The majority opinion, delivered by Justice Scalia, found a Fourth Amendment violation in the physical trespass that occurred during the placement of the GPS device on the vehicle.[167] That intrusion, wrote Justice Scalia, "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[168] The Court acknowledged that extended electronic surveillance "without an accompanying trespass" may be unconstitutional, but noted that the "present case does not require us to answer that question."[169]

In his opinion concurring in the judgment, Justice Alito criticized "the Court's reliance on the law of trespass" to decide the case.[170] Instead, he wrote, the question is whether the "respondent's reasonable expectations of privacy were violated by the long-term monitoring" of his vehicle.[171] Because "law enforcement agents tracked every movement that respondent made in the vehicle he was driving" for four weeks—a level of monitoring that Justice Alito felt impinged on reasonable expectations of privacy—Justice Alito concluded that the monitoring constituted a search.[172] Justice Sotomayor, in addition to joining the majority, provided a separate concurring opinion arguing that "the trespassory test . . . reflects an irreducible constitutional minimum."[173] Justice Sotomayor also expressed concern that the unchecked abil-

---

164. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (second alteration in original) (citation omitted).

165. *Id.* at 558, 568.

166. *Jones*, 132 S. Ct. at 949.

167. *See id.*

168. *Id.*

169. *Id.* at 953–54.

170. *Id.* at 962 (Alito, J., concurring in the judgment).

171. *Id.* at 958.

172. *Id.* at 964. Justice Alito left open the possibility that some periods of GPS surveillance might not constitute a search, but noted that in this case "the line was surely crossed before the 4-week mark." *Id.*

173. *Id.* at 955 (Sotomayor, J., concurring).

ity of the government to conduct long-term monitoring of "the sum of one's public movements" could enable it to obtain private information regarding political and religious beliefs.[174]

F. Privacy and Unmanned Aircraft Systems in Light of Supreme Court Jurisprudence

In *Ciraolo*, *Riley*, and *Kyllo*, the Supreme Court expressed a view that the extent to which an expectation of privacy is "reasonable" is tied, at least in part, to the level of technology diffusion. In addition, with respect to the specific question of the constitutionality of aerial observations, in *Ciraolo*, *Riley*, and *Dow Chemical*, the Court considered the use of public navigable airspace to be important, though not necessarily determinative. In those three rulings the Court also explicitly or implicitly distinguished overhead observations made using the naked eye or widely available camera technology from those made using less common imaging systems. For UAS privacy, these three tests—whether a technology is in general public use, whether the observations are made from public navigable airspace, and the nature of the imaging (or other information-gathering) system—will play fundamental roles.

Jones is most relevant to UAS in relation to extended surveillance. Today, tethered blimps called "aerostats" are being stationed in the sky in some places along the U.S.-Mexico border.[175] In addition, in the future, it will become practical to utilize fixed-wing unmanned aircraft for long-term surveillance. Thus, the types of constitutional questions considered (though not resolved) in *Jones* have direct implications for some categories of UAS.

---

174. *Id.* at 956.

175. Kathleen Hickey, *Former wartime blimp refitted for border surveillance*, GOV'T COMPUTER NEWS, Aug. 16, 2012, http://gcn.com/Articles/2012/08/16/CBP-aerostats-unmanned-blimps-border-surveillance.aspx.The government has increased search powers near the border. For example, within twenty-five miles of "any external boundary of the United States," 8 U.S.C. § 1357(a)(3) allows the government, without a warrant, "to have access to private lands, but not dwellings, for the purpose of patrolling the border to prevent the illegal entry of aliens into the United States."

1. *Technology in "General Public Use"*

In *Dow Chemical*, the Supreme Court wrote that warrantless "surveillance of private property by using highly sophisticated surveillance equipment *not generally available to the public*" may be unconstitutional.[176] But the Court also noted that the "photographs at issue in this case are essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them."[177]

In the *Ciraolo* ruling issued on the same day, the Court concluded that in an era when private and commercial flight is "routine," there is no reasonable expectation of privacy from naked-eye observations made from public navigable airspace.[178] The *Ciraolo* Court stopped short of stating whether or not similar overhead observations made using non-routine aircraft or imaging technology would pass constitutional muster.

Fifteen years later in *Kyllo*, the Court again viewed the extent to which a technology was publicly available as highly relevant to defining a Fourth Amendment "search." The *Kyllo* Court was clearly concerned about future developments that might enable the Government to "see" into the interior of the home from the outside.[179] This concern was reflected in the Court's expressed desire to protect people from "advancing technology" that might "discern all human activity in the home" and the resulting need to "adopt" a "rule" taking account "of more sophisticated systems that are already in use or in development."[180] Yet, in the end, the rule adopted was more narrowly crafted.

The *Kyllo* holding that a search occurs when "the Government uses a device that is not in general public use, to explore details

---

176. Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (emphasis added).

177. *Id.* at 231.

178. California v. Ciraolo, 476 U.S. 207, 215 (1986).

179. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001). Recently, there have been significant advances in "terahertz" imaging, which refers to the formation of images using electromagnetic waves with a frequency on the order of one trillion times per second. As described in a conference paper published in early 2012, researchers at University of Texas at Dallas "have designed an imager chip that could turn mobile phones into devices that can see through walls, wood, pastics, paper and other objects." *New Research Could Mean Cellphones That Can See Through Walls*, UNIV. OF TEXAS AT DALLAS NEWS CENTER, Apr. 18, 2012, http://www.utdallas.edu/news/2012/4/18-17231_New-Research-Could-Mean-Cellphones-That-Can-See-Th_article-wide.html.

180. *Kyllo*, 533 U.S. at 35–36.

of the home that would previously have been unknowable without physical intrusion"[181] clearly bars the use of uncommon technology for this purpose. However, sophisticated and uncommon are two different things. Indeed, the *Kyllo* Court called the thermal imager in question "crude"[182] while also recognizing that it was nonetheless not in general public use. Furthermore, the district court in *Dow Chemical* had found a Fourth Amendment violation, in part, because the images were taken with "the finest precision aerial camera available," permitting capture of "a great deal more than the human eye could ever see."[183] In upholding the Sixth Circuit's reversal of this decision, the Supreme Court considered the wide public availability of the camera to be more relevant than its sophistication.[184]

So how does *Kyllo* bear on the issue of "routine" technology? As the dissent in *Kyllo* noted, the Court's language raises at least the possibility that the protection offered "dissipates as soon as the relevant technology is in general public use."[185] However, to conclude from *Kyllo* that use of a widely available technology to examine a home will necessarily be constitutional is not an entirely fair reading of Justice Scalia's opinion. As Justice Scalia stated in a footnote, in response to the dissent on this specific point, thermal imaging is not routine (or at least was not in 1992, the year in which law enforcement officers used the thermal imager at issue in *Kyllo*).[186] Based on existing Supreme Court precedent, that was sufficient to find its use unconstitutional. To the extent that there is a loophole through which overhead surveillance using "routine" (and possibly but not necessarily sophisticated) technologies might slip, it was created by *Ciraolo* and *Dow Chemical*, and the Court in *Kyllo* declined to revisit it.[187]

And what about technology *not* in general public use, which at least for the moment describes the state of UAS in the United

181. *Id.* at 40.

182. *Id.* at 38.

183. Dow Chem. Co. v. United States, 476 U.S. 227, 230 (1986) (quoting Dow Chem. Co. v. United States, 536 F. Supp. 1355, 1367 (E.D. Mich. 1982)).

184. *See id.* at 238–39.

185. *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting) (internal quotation marks omitted).

186. *Id.* at 39–40 n.6 (majority opinion).

187. *See id.* ("Given that we can quite confidently say that thermal imaging is not 'routine,' we decline in this case to reexamine that factor.").

States? Under a fair reading of *Kyllo*, that fact alone would not automatically bar its use for surveillance of a home. *Kyllo* did not prevent government use of uncommon technology generally, but instead was focused on the use of such technology to "explore details of the home that would previously have been unknowable without physical intrusion."[188] Thus, although warrantless use of a UAS equipped with a sophisticated thermal imaging camera to "see" through the walls of a home would certainly run afoul of *Kyllo*, acquisition of visible-light images of a home's exterior or curtilage using a UAS-mounted consumer-grade, low-resolution imaging system in public navigable airspace would likely not. After all, the information those images would reveal could be acquired easily from manned aircraft, something that the Court has found multiple times to be constitutional. Perhaps most importantly, to the extent that a "not in general public use" test furnishes a measure of privacy protection with respect to UAS platforms, that protection inevitably will soon disappear as their use becomes more widespread.

2. *"Public Navigable Airspace"*

As is clear from *Ciraolo*, *Riley*, and *Dow Chemical*, the use of "public navigable airspace" is a threshold test for determining whether warrantless aerial observations are constitutional.[189] This does not imply that all such observations will be constitutional, but those that are made from outside public navigable airspace are almost certainly unconstitutional. The question of what constitutes "public navigable airspace" for UAS operated by the government is thus central to the privacy inquiry.

This is not as easy to answer as it might first appear. FAA regulations provide that, except as necessary for takeoff or landing, fixed-wing manned aircraft must generally operate above 1000 feet when over congested areas, and above 500 feet over most non-congested areas.[190] UAS operated above these

---

188. *Id.* at 40.

189. *See* Florida v. Riley, 488 U.S. 445, 450 (1989); California v. Ciraolo, 476 U.S. 207, 213–14 (1986); *Dow Chem. Co.*, 476 U.S. at 239.

190. 14 C.F.R. § 91.119(b)–(c) (2012). The full set of minimum altitude rules is more complex. For example, for congested areas, the minimum is 1000 feet above the highest obstacle within a horizontal radius of 2000 feet of the aircraft. § 91.119(b). For noncongested areas other than over open water or sparsely popu-

minimums therefore are certainly in public navigable airspace.[191] In addition, the altitude must always be sufficiently high to allow "an emergency landing without undue hazard to persons or property on the surface."[192]

But this is not the whole story. The FAA regulations specifically exempt helicopters[193] from the minimums if "the operation is conducted without hazard to persons or property on the surface."[194] FAA regulations nonetheless provide a *de facto* impediment to very low altitude operation of manned helicopters over residential areas: In the event of an engine failure, it would be difficult to claim that the pilot of a manned helicopter hovering fifty feet over a home could perform an emergency landing without endangering persons or property on the ground. For an unmanned helicopter (or fixed wing aircraft) weighing only a few pounds, however, the risks posed to persons on the ground by an emergency landing, though not nonexistent, are certainly modest compared to those posed by manned aircraft. Thus, the combination of the helicopter rules and the "emergency landing" provision in current FAA minimum safe altitude regulations have little or no protective power with respect to UAS privacy concerns.

An additional complicating factor is that for at least some categories of unmanned aircraft, the traditional paradigm is inverted and the FAA imposes altitude *maximums* instead of minimums. Public unmanned aircraft operated in accordance with Section 334(c)(2)(C) of FMRA must be operated at a height lower than 400 feet.[195] Unless FMRA paradoxically is read to mandate navigation outside of "navigable airspace," with respect to this class of aircraft, altitudes of 350 feet, 300 feet, and 250 feet would almost always be within public navigable airspace. However, just as

---

lated areas, the minimum is 500 feet. § 91.119(c). Over open water and sparsely populated areas, "the aircraft may not be operated closer than 500 feet to any person, vessel, vehicle, or structure." *Id.*

191. Provided, of course, that there are no other restrictions associated with the airspace.

192. § 91.119(a).

193. § 91.119(d). A helicopter is "a rotorcraft that, for its horizontal motion, depends principally on its engine-driven rotors"; a rotorcraft, in turn, is "a heavier-than-air aircraft that depends principally for its support in flight on the lift generated by one or more rotors." *Id.* § 1.1 (2012).

194. § 91.119(d).

195. FAA Modernization and Reform Act of 2012 (FMRA), Pub. L. No. 122-95, § 334(c)(2)(C), 126 Stat. 11, 77.

clearly, the air five feet above the ground in the backyard of a home is not within any reasonable definition of public navigable airspace. As the Supreme Court wrote in 1946 in *United States v. Causby*,[196] "[w]e have said that the airspace is a public highway. Yet it is obvious that if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere."[197]

Attempts to identify a precise boundary where the "immediate reaches" under the "exclusive control" of a landowner end and the area available to the public begins can lead to complex questions.[198] For example, it could be argued that a warrantless government-operated UAS that dips into a backyard at eye level to obtain photographs into the house through a back window would be operating outside of public navigable airspace, and that the images it acquired would be unconstitutional for that reason (among others).[199]

Interestingly, airspace that may not be "publicly navigable" can still be subject to governmental control. In places such as the Washington, D.C. Metropolitan Area Flight Restricted Zone, the FAA prohibits *all* outdoor flight operations (including UAS), at any altitude, unless authorized by the FAA/Transportation Security Administration.[200] Thus, the FAA can and does promulgate regulations that control the air all the way down to the ground, even over private property. However, that the government has a right to *prohibit* certain flight operations in the air a few feet above private land does not mean that the government (or a private party) has an affirma-

196. 328 U.S. 256 (1946).

197. *Id.* at 264.

198. The definition of "navigable airspace" in 49 U.S.C. § 40102 does little to resolve this question. "Navigable airspace" is defined as the "airspace above the minimum altitudes of flight prescribed by regulations under this subpart and subpart III of this part, including airspace needed to ensure safety in the takeoff and landing of aircraft." § 40102(a)(32).

199. The Supreme Court considered the more general question of whether looking into a home through a window constitutes a Fourth Amendment search in *Minnesota v. Carter*, 525 U.S. 83 (1998). In that case, police had observed of a drug transaction through a gap in the closed blinds of a window. Because the respondents "were essentially present for a business transaction and were only in the home a matter of hours," the relevant expectation of privacy was that tied to commercial premises, not residential property. As a result, the Court found that the police observations were not a Fourth Amendment violation. *Id.* at 90.

200. *See* 14 C.F.R. § 93.341 (2012).

tive right to *conduct* flight operations in that same airspace without the property owner's consent.

In the dense urban cores of cities such as New York, Chicago, and Boston, public navigable airspace can unquestionably extend *below* the level of many residences. In New York, for example, manned helicopters routinely fly over the Hudson River at altitudes significantly lower than the taller buildings in Manhattan. The air 550 feet over the Hudson River is in public navigable airspace.[201] But there is a good argument that the air six inches outside the window of a fiftieth-floor apartment in midtown Manhattan is not. As noted above, in *Causby* the Court recognized the importance of providing a landowner with "exclusive control of the immediate reaches of the enveloping atmosphere."[202] A high-rise apartment dweller should have at least as much control over the enveloping atmosphere of his or her home.[203] That control, however, will only extend a modest distance. Thus, a UAS operated at several hundred feet above the ground and at a reasonable horizontal standoff from any nearby buildings would almost always be in public navigable airspace.[204]

Will warrantless UAS surveillance from public navigable airspace always be constitutional? Certainly not. The holding in *Ciraolo* addressed naked eye observations from "public airways."[205] *Ciraolo* would provide little support for use of an imaging system capturing much more detail than could the human eye.[206] The opinions in the (slightly) more recent *Riley* decision also imply the existence of some limits. Both of the *Riley* opinions that found in favor of the government expressed concern about using operation in public navigable airspace as

---

201. Although the airspace 550 feet above the Hudson near Manhattan is publicly navigable, there are special flight rules that apply within the "Hudson River Exclusion." *See* 14 C.F.R. § 93.352 (2012). Altitudes below 1000 feet within the Hudson River Exclusion are available to aircraft conducting a "local operation" as defined in § 93.350(a).

202. *Causby*, 328 U.S. at 264.

203. An additional complication with respect to control over the air surrounding buildings in cities like New York relates to the "air rights" that are commonly transacted in association with real estate development. *See Zoning Glossary*, NEW YORK CITY DEPARTMENT OF CITY PLANNING, http://www.nyc.gov/html/dcp/html/zone/glossary.shtml#development_rights (last visited Jan. 29, 2013).

204. An exception would occur in locations subject to temporary or permanent flight restrictions.

205. California v. Ciraolo, 476 U.S. 207, 215 (1986).

206. *See id.* at 214–15.

the only threshold for constitutionality. Writing for the plurality, Justice White noted that "simply because the plane is within the navigable airspace specified by law," it does not follow that the observations it makes will always "pass muster under the Fourth Amendment."[207] Justice O'Connor also warned against relying on "compliance with FAA regulations alone,"[208] and Justice Brennan's dissent raised the same issue.[209]

Justice White's opinion in *Riley* also identifies some specific tests beyond simply being in public navigable airspace that might be applied. For example, the opinion implies that observations from legally operated aircraft that generated undue noise, wind, dust, or threat of injury could be unconstitutional.[210] Although a UAS weighing a few pounds or less would generate very little noise, wind, or dust, if it loses power it could certainly cause injuries. This could occur both directly, if it lands on a person, or indirectly, if it lands in traffic or becomes caught in power lines and initiates an injury causing event. Interestingly, the language of the opinion ties privacy expectations in part to the freedom from being subjected to a *threat* of injury, as distinct from an actual injury itself.

3. *The Role of Imaging Technology*

In *Ciraolo* and *Riley*, the aerial observations of the curtilage of a home were performed with the naked eye, a fact specifically noted by the *Ciraolo* Court[211] and by both of the *Riley* opinions that found against the government.[212] But in *Dow Chemical*, the use of a camera permitting capture of "a great deal more than the human eye could ever see" did not render the observations

---

207. Florida v. Riley, 488 U.S. 445, 451 (1989).

208. *Id.* at 453 (O'Connor, J., concurring in the judgment).

209. *Id.* at 464 (Brennan, J., dissenting).

210. *See id.* at 452 (plurality opinion).

211. "[I]t is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet." *Ciraolo*, 476 U.S. at 215.

212. Justice White's opinion stated that the investigating officer in *Riley* "circled twice over respondent's property in a helicopter at the height of 400 feet. With his naked eye, he was able to see through the openings in the roof and one or more of the open sides of the greenhouse and to identify what he thought was marijuana growing in the structure." *Riley*, 488 U.S. at 448. Justice O'Connor wrote that "I conclude that Riley's expectation that his curtilage was protected from naked-eye aerial observation from that altitude was not a reasonable one." *Id.* at 455 (O'Connor, J., concurring in the judgment).

unconstitutional; it was the public availability of the camera that mattered.[213]

What is the constitutionality of warrantless use of an extremely high-resolution (but widely available) camera on a UAS to observe the curtilage of a suspect's home? The Court has never grappled with this specific question, and existing case law is unclear on this point. A suspect could find support in *Ciraolo* and *Riley* when arguing that a Fourth Amendment violation occurred; the government could also find support in *Ciraolo* as well as in *Dow Chemical* and *Kyllo* in arguing that it did not.[214] That *Kyllo* is more recent is not dispositive in light of, among other things, the discussion of *Ciraolo* it contains.

Imaging technology is also relevant given Justice White's opinion in *Riley* that found no Fourth Amendment violation in part because "no intimate details connected with the use of the home or curtilage were observed."[215] Even though he was not speaking for a majority, Justice White's language is nonetheless intriguing, as it indicates that there may be some level of detail beyond which warrantless UAS observations, even if conducted from public navigable airspace, may cross the line into a Fourth Amendment search.

With present-day imaging capabilities, it would be an easy matter to use a UAS (or a manned aircraft) within navigable airspace to acquire imagery that includes "intimate details." For example, a government UAS at an altitude of several hundred feet could identify the topic of an electronic or paper news article being read by a person sitting in his or her fenced-in backyard. A strong case could be made that these observations, even when made from public navigable airspace, would be unconstitutional in the absence of a warrant.

---

213. Dow Chem. Co. v. United States, 476 U.S. 227, 230 (1986) (quoting Dow Chem. Co. v. United States, 536 F. Supp. 1355, 1367 (E.D. Mich. 1982)) (internal quotation marks omitted). Another key factor in *Dow Chemical* was the Court's conclusion that the observed areas were more akin to "open fields" than to the curtilage of a home. *See id.* at 239.

214. Aspects of *Ciraolo* could be cited to support both positions. A suspect could cite the reference in *Ciraolo* to "naked eye" observations. The government could in response point to the *Ciraolo* language regarding the "routine" nature of the technology of flight, which was also referenced in *Kyllo*. *See Ciraolo*, 476 U.S. at 215; Kyllo v. United States, 533 U.S. 27, 39–40 n.6.

215. *Riley*, 488 U.S. at 452.

4. *Extended Surveillance Using Unmanned Aircraft in Light of* Jones

For financial, regulatory, and logistical reasons, law enforcement agencies will usually use small UAS. Today, these platforms generally have flight durations measured in hours, rendering their continuous use for days or weeks to perform surveillance impractical. But future developments will make long-term surveillance with UAS possible. In addition, at least along the U.S.-Mexico border, aerostats already are in use today.[216]

Some of the most vexing constitutional questions will arise in association with the use of high-altitude long-endurance (HALE) UAVs. These solar-powered UAVs can stay aloft for extraordinarily long periods of time. As noted above, the QinetiQ Zephyr stayed aloft for over two weeks in a 2010 demonstration.[217] Boeing is under contract with DARPA to develop the SolarEagle, which will be able to stay aloft in the stratosphere for five continuous years.[218] Because they fly at such high altitudes, HALE UAS could potentially track every car trip in a city, or the times when lights in residences were turned on and off.[219] It will likely be much later in the decade before HALE technology becomes sufficiently advanced and cost-effective to make it practical to install a permanent HALE presence above an American city. Currently, there is no indication that any government agency plans to do so.

No Supreme Court case is directly on point with respect to the type of extended surveillance that could be performed using a HALE platform, though some of the issues involved arose in *Jones*. The *Jones* opinions contain extensive discussion of the Court's 1983 holding in *United States v. Knotts* that a "person

---

216. Hickey, *supra* note 175.

217. Chuter, *supra* note 36.

218. Press Release, Boeing Co., Boeing Wins DARPA Vulture II Program (Sept. 15, 2010), *available at* http://boeing.mediaroom.com/index.php?s=43&item=1425.

219. Satellites are not well-suited to perform extended, continuous high-resolution surveillance. The only satellites that can remain in place over one spot are in geostationary orbits, which are over 22,000 miles above the Earth—much too far to gather images revealing details of a home or curtilage. Satellites in lower orbits can acquire very detailed images, but not on a continuous basis. *See Phoenix, Tactical Technology Office*, DARPA, http://www.darpa.mil/our_work/tto/programs/phoenix.aspx (last visited Feb. 8, 2013).

traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."[220]

Justice Scalia's majority opinion in *Jones* states that performing extended surveillance "through electronic means, without an accompanying trespass" *may* be unconstitutional, "but the present case does not require us to answer that question."[221] In his concurrence in the judgment, Justice Alito expressed a view that extended electronic surveillance of public movements *is* unconstitutional, writing, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[222] Justice Sotomayor's concurrence also expressed doubts about the constitutionality of extended electronic surveillance: "I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."[223] In the end, however, it was the physical trespass involved in installing the GPS tracker, not the tracking itself, that formed the basis for the *Jones* decision.[224]

While HALE UAS surveillance is like GPS tracking in that it gathers information using technology that would have required a "large team of agents"[225] in the past, in one respect it is very different: A GPS tracker only identifies the movement of the single vehicle or other object to which it is attached, whereas HALE platforms equipped with banks of cameras could easily capture images of all the vehicle movements in an entire city. The prospect that the government might be able to capture—and then use at will—this level of information about the travels of private individuals is sobering. But if that is unconstitutional, where does that leave the networks of ground-level cameras and license plate readers that are increasingly being deployed along public streets and intersections? Those ground-level systems collect information that, when aggregated, can

220. 460 U.S. 276, 276 (1983).

221. United States v. Jones, 132 S. Ct. 945, 954 (2012).

222. *Id.* at 964 (Alito, J., concurring in the judgment).

223. *Id.* at 956 (Sotomayor, J., concurring).

224. *See id.* at 949 (majority opinion).

225. In his concurrence in the judgment in *Jones*, Justice Alito wrote that "constant monitoring of the location of a vehicle for four weeks" using traditional surveillance methods from the pre-computer age "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Id.* at 963 (Alito, J., concurring in the judgment).

track automobile trips just as thoroughly as a solar-powered HALE UAS making slow circles in the stratosphere.[226] An argument against the constitutionality of HALE systems would need to be reconciled with the information available through aggregated street-level traffic surveillance data. If government tracking of effectively all traffic in a city is unconstitutional, that holding should apply regardless of whether the technology used is on the ground or in the air.[227]

In future years it may also be necessary to revisit the assumption that widely available small, low-altitude UAS can only stay aloft for several hours. UAV Factory, a company based in Latvia, announced in the summer of 2012 that its "Penguin B" small UAS had stayed aloft for over fifty-four hours.[228] Future technological advances presumably will lead to flights of even longer durations. From a purely technological standpoint, platforms such as these conceivably could be used to survey a target for several days. Whether this is likely to happen in practice is another matter. At least under current regulations, this UAS class can only be operated by a government agency within line of sight of an operator.[229] A law enforcement agency could thus use rotating shifts of operators to fly this class of small UAS for several continuous days.

---

226. Depending on where the cameras on the aerostats along the U.S.-Mexico border are aimed, similar questions regarding long-term surveillance are raised. An important difference between aerostats and HALE UAS is the altitude. HALE platforms fly many times higher, and can survey a much larger area than can aerostats.

227. Jurisprudence related to traffic checkpoints is relevant to this issue. In *City of Indianapolis v. Edmond*, the Court noted that it "is well established that a vehicle stop at a highway checkpoint effectuates a seizure within the meaning of the Fourth Amendment." 531 U.S. 32, 40 (2000). Recording a license plate of a passing car—or tracking the car using a HALE UAS—is certainly not a seizure. However, the *Edmond* ruling also noted that "stops can only be justified by some quantum of individualized suspicion," a test that would not be met by systems that perform pervasive tracking of all vehicles in a city. *Id.* at 47.

228. *UAV Factory Touts Endurance Flight Record*, UNMANNED SYSTEMS MAGAZINE, Aug. 2012, at 13; Press Release, UAV Factor, New Endurance Record for Small Unmanned Aircraft (July 7, 2012), *available at* http://www.uvs-interntional.org/index.php?option=com_docman&task=doc_view&gid=1969&Itemid=25.

229. FAA Modernization and Reform Act of 2012 (FMRA), Pub. L. No. 112-95, § 334(c)(2)(C), 126 Stat. 11, 77.

5. *Residual Privacy Rights When a Warrant Is Obtained?*

When law enforcement officers wiretap a phone pursuant to a warrant, a great deal of privacy is lost, but ultimately some minimal privacy is still maintained. For example, a tapped phone does not provide images of the interior of a home.

But with UAS, the implication that a search warrant should have some limits is not unreasonable. Imagery acquired by UAS pursuant to a warrant could lead to profound violations of privacy for both a suspect and the other residents of a house. It is one thing for a wiretap to capture the private conversations of a suspect's spouse. It is quite another for a UAS, hovering in a backyard and taking pictures through a window (or in the future, hiding unseen inside the house), to acquire images that might show an occupant of the house in a state of undress. To assert that the government, even when armed with a warrant, has an unfettered right to acquire, store, and view such images raises significant concerns. Thus, questions of UAS privacy do not end with the issuance of a warrant.

IV. NON-GOVERNMENT UNMANNED AIRCRAFT AND THE FIRST AMENDMENT

Although much of the attention regarding UAS privacy has focused on government use and the Fourth Amendment, it is non-government use that is likely to raise some of the most significant privacy challenges in the coming years. For private entities, which are not bound by Fourth Amendment restrictions that apply to the government, the key constitutional question is the extent of their First Amendment privilege to gather information.

As the Supreme Court recognized in its 1972 *Branzburg v. Hayes* decision, "[w]ithout some protection for seeking out the news, freedom of the press could be eviscerated."[230] Furthermore, the freedom to gather information is not limited to the press. In a 2011 ruling upholding the right of a citizen to record the actions of police in a public space, the First Circuit wrote that "[i]t is firmly established that the First Amendment's aegis extends further than the text's proscription on laws 'abridging the freedom of speech,

230. 408 U.S. 665, 681 (1972).

or of the press,' and encompasses a range of conduct related to the gathering and dissemination of information."[231]

However, the freedoms conferred by the First Amendment are not unlimited. In *Branzburg*, for example, the Supreme Court recognized the existence of some bounds: "It is clear that the First Amendment does not invalidate every incidental burdening of the press that may result from the enforcement of civil and criminal statutes of general applicability."[232]

Even though almost all companies and individuals will endeavor to operate UAS responsibly, there undoubtedly exist some classes of potential UAS users who will perceive observe less restraint. If paparazzi are willing to engage in high-speed freeway chases to capture images of a celebrity,[233] it would be optimistic to the point of naïveté to expect them to always operate UAS in a manner respectful of privacy considerations and in compliance with FAA safety regulations. When, as will inevitably occur, a paparazzo or stalker flies a UAS into a backyard and takes pictures through a back window, what laws will come into play?

A. Trespassing

Common sense would suggest that a homeowner[234] has the right to prevent a UAS from being flown around his or her backyard at eye level. And indeed, in some states, trespassing statutes are worded in a manner that would encompass trespassory use of a UAS. In Arizona, for example, "entry" in association with criminal trespass is defined as "the intrusion of any part of any instrument or any part of a person's body inside the external boundaries of a structure or unit of real property."[235] Unless an argument could be made that a UAS is not an "instrument," this statute would cover intrusion by a UAS

231. Glik v. Cunniffe, 655 F.3d 78, 82 (2011).

232. 408 U.S. at 682.

233. For an example of one alleged such incident, see Kate Mather, *Photographer who allegedly chased Justin Bieber charged*, L.A. TIMES, July 26, 2012, http://articles.latimes.com/2012/jul/26/local/la-me-bieber-paparazzi-20120726.

234. Or other person legally occupying the property, such as a lessee.

235. ARIZ. REV. STAT. § 13-1501 (West 2012).

at extremely low altitudes (for example, at eye level) that are under the control of a property owner.[236]

In Oregon, by contrast, "enter" as defined in association with criminal trespass is, among other things, "[t]o enter or remain in or upon premises . . . when the entrant is not otherwise licensed or privileged to do so."[237] While this somewhat circular definition is clearly intended to criminalize unauthorized entry by a person, it leaves open the question of whether entry by a very low-flying UAS would be covered. California's trespassing laws prohibit driving a vehicle on another person's property without consent,[238] but define vehicle in a manner that excludes UAS.[239]

The general lack of attention to the potential trespassory use of UAS in current state criminal statutes is not at all surprising. In the future, it almost certainly will be necessary to add specific language to criminal trespassing statutes addressing UAS.

B. Invasion of Privacy

Use of a UAS to invade an individual's privacy could result in civil or criminal liability. With respect to civil liability, courts in most jurisdictions recognize the two forms of common law invasion of privacy most likely to arise in connection with UAS: intrusion upon seclusion and public disclosure of private

---

236. As discussed above, the question of the altitude at which a landowner's control over the air above the ground in his or her backyard ends, and the public's access begins, was at issue in *United States v. Causby*. Under any reasonable reading of *Causby* (and other relevant case law), the space in a backyard at eye level is certainly within the "immediate reaches of the enveloping atmosphere" that are under the "exclusive control" of the landowner. *See Causby*, 328 U.S. 256, 256 (1946). This interpretation is also supported by the manner in which overhanging tree branches from a neighbor's property are often handled. In many states, a homeowner has the right (subject to some exceptions) to trim tree branches in the air above his or her land. *See, e.g.*, Macero v. Busconi Corp., 12 Mass. L. Rep. 521 (Super. Ct. 2000) ("Massachusetts law recognizes a right of self-help by which a property owner can cut the limbs or branches of a tree that invade his property as long as such cutting is done at the property line.").

237. OR. REV. STAT. § 164.205(3)(a) (West 2012).

238. CAL. PENAL CODE § 602(n) (West 2012).

239. California Vehicle Code § 670, referenced in the criminal trespassing statute, defines a vehicle as "a device by which any person or property may be propelled, moved, or drawn upon a highway, excepting a device moved exclusively by human power or used exclusively upon stationary rails or tracks." CAL. VEH. CODE § 670 (West 2012).

facts.[240] In addition, some states also have civil or criminal statutes, or both, related to invasion of privacy.[241]

1. Intrusion Upon Seclusion

The potential of a UAS to intrude upon seclusion in the home is obvious. A person who is unwillingly photographed in his or her own home by a UAS hovering just outside an otherwise inaccessible window would have strong grounds for a valid cause of action. Even public figures, whose privacy rights are presumptively lower than those of private individuals,[242] can nonetheless reasonably expect views into the interior of their residences from their own backyards to be private.

Although privacy expectations are greatly reduced outside the home, the non-governmental use of a UAS to capture images and other information taken while the individual is in a public setting could nonetheless constitute an invasion of privacy. *Shulman v. Group W Productions, Inc.*,[243] a 1998 California Supreme Court ruling regarding filming that occurred following a car accident, is instructive in this regard. In *Shulman*, the victims of an accident were captured on video and audio recording, without their consent, for a television program called *On Scene: Emergency Response*.[244] The recording occurred both at the scene of the accident as well as in a rescue helicopter during transport to a hospital.[245]

The California Supreme Court affirmed the court of appeals' decision to reverse the trial court's summary judgment finding that the television program producers' activities were protected

---

240. Prosser articulated four forms of the common law invasion of privacy tort in 1960: (1) "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs;" (2) "[p]ublic disclosure of embarrassing private facts about the plaintiff;" 3) "[p]ublicity which places the plaintiff in a false light in the public eye;" and 4) "[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness." William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); *see also* RESTATEMENT (SECOND) OF TORTS §§ 652A–652E (1997).

241. *See, e.g.*, CAL. CIV. CODE § 1708.8 (West 2011); N.J STAT. ANN. §§ 2C:14-9, 2A:58D-1 (2004).

242. *See generally* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974); New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

243. 955 P.2d 469 (Cal. 1998).

244. *Id.* at 475.

245. *Id.* at 474–75.

under the First Amendment.[246] The court held that a woman injured in the accident "was entitled to a degree of privacy in her conversations with [the nurse] and other medical rescuers at the accident scene."[247] It was improper, the ruling stated, to conclude that the "plaintiffs had no reasonable expectation of privacy at the accident scene itself because the scene was within the sight and hearing of members of the public."[248] At the time of the rescue, the vehicle was located "in a ditch many yards from and below" a highway, rendering it "unlikely . . . that any passersby on the road could have heard" the conversation of the victim with the nurse and other rescuers.[249]

The *Shulman* decision provides important guidance regarding newsgathering and UAS with respect to intrusion upon seclusion by drawing a distinction between the information about a newsworthy event available to passersby and the potentially greater amount of information available only to those intimately involved in the event itself. Under some circumstances, there will be no difference: If a crowd of people has gathered around an assault victim who is being treated by paramedics, the conversation between the victim and the paramedics may well be audible to all, and the victim's reasonable expectation of privacy correspondingly lower. But there will be many cases in which, as in *Shulman*, passersby have far from complete information about an unfolding event. Using a UAS to fill in the gaps would carry a risk of crossing the line into intrusion.

Just as the First Amendment does not provide an impenetrable shield for all uses of video, audio, and other electronic monitoring in public areas, intrusion upon seclusion is not automatically implicated for all observations of activities occurring in a home. A passerby on the street at night who happens to glance up and notice that the light in a nearby home has just been turned off is certainly not violating privacy rights. Likewise, courts will be very unlikely to consider a fleeting, acci-

246. *See id.* at 497–98.

247. *Id.* at 491.

248. *Id.*

249. *Id.* In addition to considering whether the audio and video recorded at the scene of the accident intruded on the victim's expectation of privacy, the California Supreme Court also considered the recording that took place within the helicopter, ruling that the "Court of Appeal correctly found [that] triable issues exist as to whether defendants invaded plaintiffs' privacy by accompanying plaintiffs in the helicopter." *Id.* at 477.

dental capture of imagery of a home's curtilage or (through a window) interior acquired by a passing UAS to be an invasion of privacy. Although the specifics vary from state to state, to prevail in a common law or statutory intrusion upon seclusion claim, a plaintiff generally must establish, at a minimum, that the intrusion was intentional and that it would be "highly offensive to a reasonable person."[250]

Some highly offensive intrusions upon seclusion have nonetheless been protected under the First Amendment. Most notably, in *Snyder v. Phelps*[251] the Supreme Court ruled in favor of members of the Westboro Baptist Church who had picketed the funeral of a serviceman killed in Iraq. A jury in Maryland had found members of Westboro Baptist Church liable for damages based on claims including intrusion upon seclusion.[252] However, in affirming the Fourth Circuit's reversal, the Supreme Court ruled that "the First Amendment bars Snyder from recovery for intentional infliction of emotional distress or intrusion upon seclusion" against Westboro Baptist Church members and that "we must likewise hold that Snyder cannot recover for civil conspiracy based on those torts."[253]

2. *Publication of Private Facts*

Precedents from state court rulings unrelated to aviation indicate that UAS could also figure into invasion of privacy through the publication of private facts. This could be particularly important with respect to UAS images of private individuals who become involuntarily caught up in newsworthy events.

In September 1999, *Sports Illustrated* published a story entitled "Every Parent's Nightmare" that included a photograph of a Little League team.[254] There were eighteen people in the photograph, including a team manager who had been convicted of molestation

---

250. Restatement (Second) of Torts § 625B (1977).

251. 131 S. Ct. 1207 (2011).

252. *Id.* at 1214. The District Court reduced the damages award but left the verdict intact. *Id.*

253. *Id.* at 1220.

254. William Nack & Don Yaeger, *Every Parent's Nightmare*, SPORTS ILLUSTRATED, Sept. 13, 1999, at 40, 42–43, *available at* http://sportsillustrated.cnn.com/vault/edb/reader.html?magID=SI&issueDate=19990913&mode=reader_vault.

charges in 1971 and who pled guilty in April 1998 to charges of molesting five of the children he coached in Little League.[255]

Ten of the people in the photograph filed suit against Time Warner, Inc., the then-owner of *Sports Illustrated*, for invasion of privacy and infliction of emotional distress.[256] In 2001, the California Court of Appeal upheld a lower court decision to deny Time Warner's motion to strike the complaint, writing that the "plaintiffs have demonstrated a prima facie case for invasion of privacy," particularly in relation to public disclosure of a private fact.[257] The court recognized that while the identity of the molester was publicly known and certainly newsworthy, the identities of the other coaches and the players on the team were not.[258]

Publication of private facts via imagery was also at issue in a Florida case involving a woman who suffered from a poorly performed plastic surgery.[259] The woman consented to be interviewed for a television program under the condition that the video would be edited to alter her voice and obscure her face.[260] When the broadcast took place without these two things occurring as promised, thereby revealing her identity, she filed suit.[261] In reversing a summary judgment in favor of the defendant, the Florida Court of Appeals held that "while the topic of the broadcast was of legitimate public concern, the plaintiff's identity was not."[262]

Images acquired by UAS could easily convey facts not previously known to the public, and, upon publication, could be an actionable invasion of privacy in many states. While news organizations are well aware of the tension between the privacy rights of their subjects and the organizations' First Amendment right to gather news, they will almost certainly need to reexamine existing policies in light of the unique imaging and other information gathering capabilities (such as monitoring of wire-

---

255. *Id.* at 43.

256. M.G. v. Time Warner, Inc., 89 Cal. App. 4th 623, 626 (2001).The same photograph had also been broadcast on the HBO program *Real Sports*. HBO was also owned by Time Warner.

257. *Id.*

258. *Id.* at 632.

259. Doe v. Univision Television Grp., Inc., 717 So. 2d 63, 64 (Fla. Dist. Ct. App. 1998).

260. *Id.*

261. *Id.*

262. *Id.* at 65.

less signals) of UAS. In addition, given the ease with which anyone—not only news organizations—can now publish content, all users of UAS who contemplate publishing aerial images or other information from UAS would be well advised to give careful consideration to the common law and statutory invasion of privacy frameworks that apply in their jurisdictions.

C. Stalking and Harassment

In January 2009, the U.S. Department of Justice released a report based on data collected from over three million stalking victims and two million harassment victims.[263] About 245,000 of the stalking victims and 70,000 of the harassment victims stated that they had been subjected to electronic monitoring using one or more of the following devices: video or digital cameras, computer spyware, listening devices, and GPS tracking.[264] Stalkers will have no qualms about adding UAS to this list.

It was not until 1990 that California became the first state to criminalize stalking.[265] Today, statutes addressing stalking (and typically harassment) are now on the books in all fifty states and in Washington, D.C. Fortunately, many of these statutes are worded broadly enough that use of a UAS to persistently follow a person or peer into his or her car or home would be considered, at the very least, harassment. Stalking often carries the additional connotation of causing the victim to fear for his or her safety.[266] Under some circumstances, UAS use alone could constitute stalking (for example, if it is used to chase or corner a person).[267] More often, a stalker using a UAS would also be engaged in a larger constellation of behaviors consistent with stalking. To the extent that anti-harassment and anti-stalking statutes specifi-

---

263. Katrina Baum et al., U.S. Dep't. of Justice, Bureau of Justice Statistics Special Report, Stalking Victimization in the United States (2009), http://bjs.ojp.usdoj.gov/content/pub/pdf/svus.pdf.

264. *Id.* at 5.

265. *See* Christine B. Gregson, Comment, *California's Antistalking Statute: The Pivotal Role of Intent*, 28 GOLDEN GATE U. L. REV. 221, 221 (1998).

266. *See, e.g.*, CAL. PENAL CODE § 646.9 (West 2008): "Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking . . . ."

267. Obviously, the other requirements of the legal definition of stalking must be met. As such, a child who momentarily chases his or her sibling using a 9-ounce toy remote control helicopter is clearly not engaging in stalking.

cally enumerate the technologies that might be exploited, UAS should be added to the list. If a stalker employing a UAS crosses state lines (or operates a UAS, with the assistance of someone local to the victim, from a different state), then federal anti-stalking statutes could also be implicated.[268]

D. Unmanned Aircraft and Business Privacy

In 2011, a Texas man flew an unmanned aircraft over land near a Dallas-area meat packing plant and acquired images appearing to show environmental violations.[269] He contacted the Coast Guard, and in early 2012 the Texas Environmental Crimes Task Force served a search warrant on the company.[270] Once on the property, investigators found a pipe that "originate[d] in the back of the slaughterhouse" that appeared to be channeling pigs' blood into a nearby river and "[was] not linked to a waste water system."[271]

Though few would rush to defend a slaughterhouse that may be in violation of environmental codes, the ability of private citizens or groups to easily inspect for such violations via overflights raises complex issues. To the extent that such overflights are lawfully conducted and reveal activities that may be endangering public health, they are obviously valuable. But what happens if a well-meaning but overzealous environmental group conducts daily flights over a large, fenced-in manufacturing facility and repeatedly reports "violations" to the government that turn out, after costly and time-consuming on-the-ground inspections, not to be violations after all? Does the company that owns the facility have grounds to ask a court to enjoin the environmental group from further overflights? What if the group posts pictures from its daily aerial surveillance missions on the Internet, and in doing so exposes information that the company regards as a trade secret? Could the group use a UAS to examine the interior of buildings at the facility using an advanced thermal imager that, if in government

---

268. *See, e.g.*, 18 U.S.C. §§ 2261, 2261A, 2262, 2265 (2006).

269. Meghan Keneally, *Drone plane spots a river of blood flowing from the back of a Dallas meat packing plant*, MAILONLINE, Jan. 24, 2012, http://www.dailymail.co.uk/news/article-2091159/A-drone-plane-spots-river-blood-flowing-Dallas-meat-packing-plant.html.

270. *Id.*

271. *Id.*

hands and used to inspect a home, would be unconstitutional under *Kyllo*? More generally, to what extent does a corporation have common law or constitutional privacy rights that parallel those accorded to individuals?

This last question was raised but not fully resolved in a recent Supreme Court case, *FCC v. AT&T, Inc.*[272] While noting that "this case does not call upon us to pass on the scope of a corporation's 'privacy' interests as a matter of constitutional or common law,"[273] the Court ruled that the "protection in [the Freedom of Information Act] against disclosure of law enforcement information on the ground that it would constitute an unwarranted invasion of personal privacy does not extend to corporations."[274] The Court also expressed skepticism regarding arguments that corporations have a common law right to personal privacy, writing that "[o]n the contrary, treatises in print around the time that Congress drafted the exemptions at hand reflect the understanding that the specific concept of 'personal privacy,' at least as a matter of common law, did not apply to corporations."[275] Corporate privacy rights are related in part to the much broader question regarding the extent to which constitutional protections extend to corporations.[276] UAS represent one of the many ways in which those rights may be tested in the coming years.

The fact that UAS might be used to perform corporate espionage is another important issue. Observations of a competing company's facilities and activities—whether made from the ground or the air—are not necessarily illegal. For example, consider a person who drives by a competing company on public roads as part of his or her regular commute to work. If this person notices that there are suddenly far fewer cars in the company's parking lot than in previous months, he or she might infer that there have been significant layoffs. Under this scenario, visual observations have yielded potentially valuable information about a competitor without breaking any laws. Analogous scenarios involving incidentally acquired UAS imagery can also be envisioned.

---

272. 131 S. Ct. 1177 (2011).
273. *Id.* at 1184.
274. *Id.* at 1185.
275. *Id.* at 1183–84.
276. *See, e.g.*, Citizens United v. FEC, 558 U.S. 310 (2010).

By contrast, circling a UAS over the roof of a competing company to intercept wireless signals emanating from the building would represent something similar to an "illegal wiretap" and violate the Stored Communications Act.[277] Photographs taken from a UAS without authorization that both (1) convey a trade secret, and (2) are obtained for the purpose of benefiting a "foreign government, foreign instrumentality, or foreign agent" would violate economic espionage statutes.[278]

V. NEW FRAMEWORKS FOR UNMANNED AIRCRAFT SYSTEMS AND PRIVACY

Many of the most important UAS privacy questions relate directly to the scope and interpretation of the First and Fourth Amendments. Those questions will be addressed in the inevitable court tests that will arise with increased UAS use. But there are also proactive steps that can be taken, including the adoption of voluntary policies by law enforcement agencies as well as new federal, state, and local legislation.

A. Voluntary Approaches

Several voluntary approaches for addressing UAS privacy have been proposed. These include the Association for Unmanned Vehicle Systems International (AUVSI) Code of Conduct, which calls for a commitment to "respect the privacy of individuals,"[279] as well as a set of model guidelines released by the International Association of Chiefs of Police (IACP).[280]

Although the IACP guidelines are not binding, many American law enforcement agencies likely will adopt the guidelines or use them as a starting point to develop more extensive guidelines. The IACP guidelines recommend that "[w]here there are specific and articulable grounds to believe that the UA [unmanned aircraft] will collect evidence of criminal

277. *See* 18 U.S.C. § 2511(1)(a) (2006).

278. *See, e.g.*, 18 U.S.C. § 1831(a)(2) (2006).

279. *Unmanned Aircraft System Operations Industry "Code of Conduct"*, ASS'N FOR UNMANNED VEHICLE SYS. INT'L, www.auvsi.org/conduct/ (last visited Feb. 1, 2013).

280. *Recommended Guidelines for the use of Unmanned Aircraft*, INT'L ASS'N OF CHIEFS OF POLICE: AVIATION COMM. http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf (last visited Feb. 1, 2013).

wrongdoing and if the UA will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight."[281] The guidelines also address data minimization, community involvement and feedback regarding policies for UAS use, and documentation of UAS flights.[282] Some of these recommendations are consistent with recommendations provided by the American Civil Liberties Union in a December 2011 report on "Protecting Privacy From Aerial Surveillance."[283] Voluntary frameworks will play a vital role in addressing UAS privacy concerns both directly, in terms of encouraging law enforcement agencies to use UAS responsibly, and indirectly, by spurring an important dialog between law enforcement agencies and their communities.

B. Federal Legislation

There were multiple bills related to UAS privacy introduced in the 112th Congress, though none were enacted.[284] In June 2012, Senator Rand Paul introduced the "Preserving Freedom from Unwarranted Surveillance Act of 2012,"[285] a bill that, subject to a small number of exceptions (such as preventing "imminent danger to life"), would have required a warrant for gov-

---

281. *Id.* at 3.

282. *Id.* at 2–3. In the context of privacy, "data minimization" refers to the practice of collecting only relevant information, and destroying data that has ceased to become relevant. *See, e.g.*, ANDREAS PFITZMANN, MARIT HANSEN, & HANNES TSCHOFENIG, INTERNET ENGINEERING TASK FORCE, TERMINOLOGY FOR TALKING ABOUT PRIVACY BY DATA MINIMIZATION: ANONYMITY, UNLINKABILITY, UNDETECTABILITY, UNOBSERVABILITY, PSEUDONYMITY, AND IDENTITY MANAGEMENT (2010), http://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html.

283. *See* Jay Stanley & Catherine Crump, Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft, Am. Civil Liberties Union 15–16 (2011), http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf.

284. Some of these UAS privacy legislative initiatives, as well as more general Fourth Amendment UAS issues are discussed in Richard M. Thompson II, Cong. Research Serv., R42701, Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses (2012), *available at* http://www.fas.org/sgp/crs/natsec/R42701.pdf.

285. Preserving Freedom from Unwarranted Surveillance Act of 2012, S. 3287, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/s3287. Essentially the same bill was introduced in the House by Representative Austin Scott. *See* Preserving Freedom from Unwarranted Surveillance Act of 2012, H.R. 5925, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/hr5925.

ernment use of UAS to "gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation."[286] A week later, Representative Shelley Capito introduced H.R. 5961, which would have limited "aerial surveillance of agricultural land."[287] The next month, Representative Ted Poe introduced the "Preserving American Privacy Act of 2012,"[288] which would have prohibited the use of UAS "for law enforcement purposes or for surveillance of a United States national or real property owned by that national . . . except pursuant to warrant and in the investigation of a felony."[289]

In December 2012, Representative Edward J. Markey introduced the "Drone Aircraft Privacy and Transparency Act of 2012." The bill would have required all entities seeking a "grant of authority to operate an unmanned aircraft system in the national airspace system" to provide a "data collection statement" specifying, among other things, "whether the unmanned aircraft system will collect information or data about individuals or groups of individuals," and if so, how it will be used.[290] Applications from law enforcement agencies would also have had to provide a "data minimization statement" describing the agencies' policies for minimizing data collection unrelated to a crime investigation and "requir[ing] the destruction of such information and data, as well as of information and data collected by the unmanned aircraft system that is no longer relevant to the investigation of a crime under a warrant."[291] With some exceptions for exigent circumstances, the bill would also have required law enforcement agencies to obtain a warrant for "generalized surveillance."[292]

There will undoubtedly be a new set of UAS privacy bills and privacy related amendments introduced (or reintroduced) in the 113th Congress and beyond. It is relatively easy to draft

---

286. *Id.*

287. Farmer's Privacy Act of 2012, H.R. 5961, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/hr5961.

288. Preserving American Privacy Act of 2012, H.R. 6199, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/hr6199.

289. *Id.* § 2.

290. Drone Aircraft Privacy and Transparency Act of 2012, H.R. 6676, 112th Cong. § 339 (2012), *available at* http://www.govtrack.us/congress/bills/112/hr6676/text.

291. *Id.* § 339(c).

292. *Id.* § 341.

legislative language that will increase privacy from UAS observations. It is far harder to do so without negatively impacting the use of UAS in applications that raise few or no privacy concerns. For example, as part of an arson investigation, police might want to employ a UAS to acquire overhead images of a formerly vacant industrial building that has been damaged by a suspicious fire. Requiring police to first obtain a warrant would delay the investigation and increase the burden on the courts with no benefit to privacy.

When drafting legislation, it is also important to consider the role that could be played by unintentionally captured images. Suppose that a brutal assault that takes place on a sidewalk is captured on video by a government-operated UAS that happens to be monitoring traffic on the adjacent street. Suppose further that the video from the UAS turns out to be the only available evidence that can identify the perpetrator. It would defy common sense if the police or prosecutors were barred by new UAS privacy rules from making use of this information.

Legislation that would include a blanket prohibition on government use of private UAS data in criminal investigations would also be ill advised, as well as inconsistent with what routinely occurs in nonaviation settings. Investigators often use images collected from privately owned surveillance cameras to help solve crimes, including, in many cases, cameras that were not owned or operated by the victim of the crime. In June 2012, a man suspected of killing three people in New York was arrested thanks in large part to images captured by a surveillance camera down the street from the scene of the crime.[293] What mattered most was that the camera captured the images vital to identifying the suspect, not whether it was publicly or privately owned. If, in the example in the previous paragraph, the images of the assault on the street had been captured by a UAS operated by a television station instead of by the government, it would make no sense to place them beyond the legal reach of investigators.

Any new legislation should also recognize that images of public spaces from government (or private) UAS will sometimes also include images of nearby homes. Residences next to a freeway are often within the frame of view of video from

293. *Police arrest suspect accused of executing three men outside Columbia University*, MAILONLINE, June 23, 2012, http://www.dailymail.co.uk/news/article-2163776/Police-arrest-suspect-accused-executing-men-outside-Columbia-University.html.

manned traffic helicopters reporting on a freeway problem. Video from UAS used to monitor traffic will be no different. Thus, a law stating that no UAS images of any nonpublic spaces can ever be acquired by the government without a warrant would, at least on its face, effectively ban government UAS use in almost any suburban or urban setting.

UAS privacy legislation, either at the federal or state level, should also avoid creating collateral damage for the operation of model aircraft. The Academy of Model Aeronautics, which, with over 150,000 members,[294] constitutes the world's largest model aviation organization, has an exemplary seventy-five-year safety record and a safety code that requires pilots of radio-controlled model airplanes to "avoid flying directly over unprotected people, vessels, vehicles or structures."[295] Aircraft operated in this manner are ill-suited for surveillance. Impeding their operation in the name of privacy would benefit no one.

"Drone" hobbyists should similarly be protected from legislation that leaves them as collateral damage. If, five years from now, a parent and child acting in compliance with applicable FAA regulations wish to fly a very small UAS in a backyard or public park, new privacy laws should not force the parent to file paperwork with the government documenting the date, time, duration, location, and image collection status of every flight.

As is clear from the above, there is no shortage of unsuitable legislative approaches. The best solutions are those that increase privacy protections without impeding reasonable, non-privacy-violating uses. Laws addressing data retention by government UAS users are one possible example. It is also reasonable to require law enforcement agencies to keep thorough records identifying the details of flight operations, including the date and time, location, who was operating the aircraft, and what sort of data was collected.[296]

---

294. *What is AMA?*, ACAD. MODEL AERONAUTICS, http://www.modelaircraft.org/files/102.pdf (last visited Feb. 1, 2013).

295. *Academy of Model Aeronautics National Model Aircraft Safety Code* para. B(1), ACAD. MODEL AERONAUTICS, http://www.modelaircraft.org/files/105.pdf (last visited Feb. 1, 2013).

296. Laws specifically addressing UAS image data retention would raise the issue of consistency with respect to retention of data from ground-level, government-operated surveillance cameras.

C. *State and Local Legislation and the Scope of Federal Preemption*

The prospect of state and local UAS privacy regulation raises the issue of federal preemption.[297] Higher courts have repeatedly ruled that aircraft safety regulation has been preempted by the federal government. In 2007, the Ninth Circuit held that "[t]he [Federal Aviation Act] and regulations promulgated pursuant to it establish complete and thorough safety standards for air travel, which are not subject to supplementation by, or variation among, state laws."[298] Similarly, a 1999 Third Circuit ruling stated "[b]ecause the legislative history of the FAA and its judicial interpretation indicate that Congress's intent was to federally regulate aviation safety, we find that *any* state or territorial standards of care relating to aviation safety are federally preempted."[299]

Aircraft noise is another aviation-related field that has been federally preempted. In a 1973 decision involving Burbank's right to establish an airport curfew to address noise concerns, the Supreme Court ruled that the federal government "has full control over aircraft noise, preempting state and local control."[300] And in 1978, the Airline Deregulation Act included an express preemption prohibiting states from enacting laws "related to a price, route, or service of an air carrier that may provide air transportation."[301]

Yet this does not prevent states from passing any laws relating to how aircraft are flown. Reckless operation of aircraft is

---

297. As the Supreme Court explained in a 1987 ruling, "when acting within constitutional limits, Congress is empowered to pre-empt state law by so stating in express terms." Cal. Fed. Sav. & Loan Ass'n v. Guerra, 479 U.S. 272, 280 (1987). In addition, "congressional intent to pre-empt state law in a particular area may be inferred where the scheme of federal regulation is sufficiently comprehensive to make reasonable the inference that Congress 'left no room' for supplementary state regulation. . . . As a third alternative, in those areas where Congress has not completely displaced state regulation, federal law may nonetheless pre-empt state law to the extent it actually conflicts with federal law." *Id.* at 280–81 (citation omitted).

298. Montalvo v. Spirit Airlines, 508 F.3d 464, 468 (9th Cir. 2007).

299. Abdullah v. Am. Airlines, 181 F.3d 363, 371 (3d Cir. 1999).

300. City of Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624, 633 (1973).

301. 49 U.S.C. § 41713(b)(1) (2006); *see also* John Maggio & Allison M. Surcouf, *Federal Preemption in The Field of Aviation*, 78 J. TRANSP. L., LOGISTICS & POL'Y 243, 249–50 (2011).

prohibited by both FAA regulations[302] and criminal statutes in many states. In ruling that a Maryland law making it a crime to "operate an aircraft . . . in a careless or reckless manner so as to endanger the life or property of another"[303] was not preempted by federal law, the Maryland Court of Appeals wrote that it "would be incongruous indeed, in light of the federal purposes and objectives, if Maryland were to be constitutionally precluded from the criminal prosecution of a person for such conduct because a federal regulation authorized civil penalties."[304] More generally, the court observed, "[w]e have no difficulty whatever in deciding that Congress has not occupied the entire field of aeronautics by the Federal Aviation Act of 1958."[305] Thus, federal preemption is complex both generally[306] and with respect to aviation.[307]

A state does not have the authority to enact UAS privacy laws that would decrease the safety of flight operations. A state law aiming to prevent UAS from hovering for too long over a home by requiring a certain minimum speed would raise concerns with respect to airspace safety, and would be unlikely to withstand a legal challenge. On the other hand, although it would be unadvisable, a state or municipality could enact legislation forbidding the use of any public funds to purchase or operate unmanned aircraft. There is also a gray area between these two extremes. State laws attempting to limit where and how government UAS can be operated, the resolution of the cameras they carry, or the retention of the data they collect would almost certainly be subject to preemption challenges.

From a preemption standpoint, the safest legislative role for states with respect to UAS privacy lies in minimizing privacy abuses by non-government UAS operators. State power to address trespass, invasion of privacy, harassment, and stalking is well established. Current civil and criminal statutes in those areas were drafted in an era, which is now ending, when UAS

---

302. 14 C.F.R. § 91.13 (2006).

303. Ward v. State, 374 A.2d 1118, 1118 (Md. 1977) (quoting MD. ANN. CODE. art. 38, § 1 (1971), *repealed by* Acts 2004, Ch. 26, § 1 (2004)).

304. *Id.* at 1125.

305. *Id.* at 1123–24.

306. See Geoffrey C. Hazard, Jr., Quasi-Preemption: Nervous Breakdown in Our Constitutional System, 84 TUL. L. REV. 1143, 1145 (2010).

307. *See* Maggio & Surcouf, *supra* note 301, at 243.

were not widely accessible to private citizens. As a result, in many cases these laws fail to anticipate some of the unique ways in which UAS in the hands of irresponsible operators could be used to threaten privacy. These statutes should be reexamined to identify and close any loopholes that might be exploited.

State UAS privacy regulations also run the risk of being undermined by the physics and geometry of flight. Consider a UAS operated over Maryland, at the Virginia border, and at a high enough altitude to obtain very precise imagery of activities in Virginia five miles south of the Potomac River.[308] While the operators of the UAS would certainly need to comply with federal and Maryland laws, they could very credibly argue that their data collection practices should not be subject to Virginia law.[309] The scenarios that could play out in relation to municipal-level regulations are even more varied. If Berkeley, California, were to prohibit its police department from purchasing or using UAS, a UAS owned and operated by the City of Oakland, which is adjacent to Berkeley, could easily remain over Oakland while acquiring video of portions of Berkeley. The Oakland UAS could also freely cross into the airspace over Berkeley.

The early months of 2013 have seen a significant increase in UAS-related legislative activity at the state and local levels. To cite some of the many examples, in February 2013 the Virginia General Assembly passed a bill that, if signed into law by the Governor, would place broad restrictions on state and local law enforcement UAS use until July 2015.[310] An Oregon Senate bill, if enacted, would prohibit certain UAS uses within what it defines as the "Airspace of Oregon"; that is, "the space above the ground that is not part of airspace governed by federal law." [311]

---

308. In this hypothetical scenario, it is assumed that the flight would occur outside the restricted zone in the Washington, D.C., area. *See Notice to Airmen 0/8326*, FED. AVIATION ADMIN., http://tfr.faa.gov/save_pages/detail_0_8326.html (last visited Feb. 1, 2013).

309. The ability of state law to reach high into the sky is questionable even in its "own" airspace. It is doubtful, for example, that a state could enact a valid law prohibiting passengers in commercial airliners flying over the state at 36,000 feet from taking pictures through the aircraft windows of the scenery below.

310. Jason Koebler, *Virginia Becomes First State to Pass Drone Regulations*, US NEWS, Feb. 5, 2013, http://www.usnews.com/news/articles/2013/02/05/virginia-becomes-first-state-to-pass-drone-regulations-.

311. S.B. 71, 77th Legis. Assemb., Reg. Sess. (Or. 2013), *available at* http://www.leg.state.or.us/13reg/measures/sb0001.dir/sb0071.intro.html.

Other states in which UAS-related measures have been introduced include California,[312] Florida,[313] and Texas.[314]

CONCLUSION

The only certain aspect of the debate about unmanned aircraft and privacy is that it will be contentious. Some people believe that there is no need to create new laws,[315] whereas others believe that UAS "could be just the visceral jolt society needs to drag privacy law into the twenty-first century."[316]

In the quarter of a century since *Ciraolo*, the cost of sophisticated imaging technology has plummeted. UAS will make it easy to put that technology in the air. Thus, the constitutionality of government UAS observations of a home or its curtilage using imaging technology that is both sophisticated and in general public use is certain to be tested.

None of the key Supreme Court precedents definitively resolve this issue. *Ciraolo* and *Riley* involved naked eye observations. *Dow Chemical* involved a camera that was both widely available and sophisticated for its time, but did not concern a home or curtilage. In *Kyllo*, the Court considered the thermal imager to be non-routine. And *Jones* concerned GPS, not imaging.

In combination, however, these rulings indicate that the Fourth Amendment is likely to provide significantly more protection from government UAS observations than is commonly assumed. At the very least, the Court will not grant the government the unconstrained power to perform warrantless UAS surveillance. Instead, the Court is more likely to adopt a test tied to the amount of detail revealed as opposed to the level of technology diffusion. Under that standard, even unsophisticated imag-

---

312. S. B. 15, 2013–2014 Legis., Reg. Sess. (Cal. 2013), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0001-0050/sb_15_bill_20121203_introduced.html.

313. S.B. 92, 2013–2014 Legis., Reg. Sess. (Fla. 2013), *available at* http://www.flsenate.gov/Session/Bill/2013/0092/BillText/Filed/PDF.

314. *See* Robert Stanton, *Bill wants to make sure drone owners aren't neighborhood spies*, HOUSTON CHRONICLE, Feb. 6, 2013, http://www.chron.com/news/houston-texas/houston/article/Bill-wants-to-make-sure-drone-owners-aren-t-4256365.php.

315. *E.g.*, Jim Harper, *Old Laws Can Cover New Technologies*, N.Y. TIMES, Feb. 22, 2012, http://www.nytimes.com/roomfordebate/2012/02/20/civilian-drones-in-the-united-states/old-laws-can-cover-new-technologies.

316. M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 29 (2011), http://www.stanfordlawreview.org/online/drone-privacy-catalyst.

ing technology might lead to a Fourth Amendment violation if it is misused in a low-flying government UAS, while images from a sophisticated camera flown at a high altitude might reveal very few details and raise no constitutional concerns.

When considering potential new statutory UAS privacy protections, it is helpful to keep in mind what has occurred with the Internet and mobile telephones, two technologies that are associated with privacy threats that are in some respects much more significant than those that will arise from unmanned aircraft. Both the Internet and mobile phones grew as fast as their underlying technologies enabled. As a result, the public and legislative dialogue regarding how best to address the privacy issues they raise has been conducted with a strong appreciation of their benefits. By contrast, while the privacy concerns associated with domestic UAS are real and deserving of attention, they are getting significant focus long before the potential benefits of the technology are widely recognized.

This early consideration creates both opportunities and risks. The opportunities lie in the ability to proactively address the privacy issues associated with a new technology before it becomes common. The risks lie in letting this information imbalance—in which the privacy downsides are well-known but the benefits are not—lead to correspondingly imbalanced legislative approaches.

If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.

Thus, while it is important to proactively consider how to protect against the privacy abuses UAS could make possible, in doing so it is important to recognize the near impossibility of predicting all of the ways that a rapidly developing technology can be used—for good or for ill—in future years. Maintaining that perspective will be vital in achieving good UAS policy outcomes.

12 Alaska L. Rev. 1

*1 WELCOME TO THE "LAST FRONTIER," PROFESSOR GARDNER: ALASKA'S INDEPENDENT APPROACH TO STATE CONSTITUTIONAL INTERPRETATION

Alaska Law Review

June, 1995

Ronald L. Nelson[a1]

This article rebuts recent criticism of efforts by state supreme courts to interpret state constitutional provisions differently than the United States Supreme Court interprets analogous provisions in the United States Constitution. This area of law, sometimes called New Judicial Federalism, has been the subject of considerable comment over the last twenty years. By focusing on equal protection, privacy, religious freedom and access to natural resources, the article examines Alaska's unique constitutional background and independent interpretation. This analysis of Alaskan constitutional rights reveals a viable and active brand of New Judicial Federalism. The article concludes that Alaska's independent approach to state constitutional law is an example of a constitutional discourse that is both uniquely local and nationally valuable.

Ronald L. Nelson, *Welcome to the "Last Frontier," Professor Gardner: Alaska's Independent Approach to State Constitutional Interpretation*, 12 Alaska L. Rev. 1 (1995)

. . .

B. Privacy

Alaska's right to privacy, particularly in the non-criminal context, has undergone development similar to Alaska's equal protection doctrine.[82] In fact, this right to privacy may be one of the most well-known indicators of Alaska's judicial independence. While the right to privacy is now embodied in a specific provision of the state constitution, it was not included in the original Declaration of Rights. Instead, article I, section 22 was added to the constitution in 1972. Prior to 1972, the right to privacy was viewed by most state courts as a matter of federal protection and not routinely addressed at the state level. In the federal courts, however, the concept was not well-defined and was found primarily in the right "to be let alone," the right of marital privacy, the privacy of the home, or some other penumbral definition.[83]

In 1972, the Alaska Supreme Court addressed the privacy issue when it decided a pre-amendment case, *Breese v. Smith*.[84] Breese involved a challenge by a student to school hair length regulations. After examining federal privacy protection and various state and federal cases, the court decided not to resolve the case on federal grounds because of the unsettled state of the privacy issue at the federal level. The Breese court instead decided that "avoidance of *18

the federal thicket [was] the better course,"[85] and struck down the regulations on independent state grounds. Citing a general liberty right under article I, section 1 of the state constitution,[86] and noting the state's duty to open and maintain public schools,[87] the court found that the student had a "fundamental . . . right to select [his] own individual hair style[ ] without governmental direction."[88] It then determined that the state's interest in maintaining the regulation was insufficiently "compelling" to overcome the student's privacy right.[89]

The *Breese* court examined cases from federal and state courts as well as notes and articles by various commentators.[90] Citing *Roberts v. State*[91] and *Baker v. City of Fairbanks*,[92] the court characterized its decision as a matter of fulfilling its judicial obligation to move forward and develop additional rights under the state constitution without being constrained by federal decisions.[93] *Breese* therefore set the stage for the development of the right to privacy law under the explicit language of section 22.

In 1975 the Alaska Supreme Court decided the first major case under the 1972 privacy amendment. In *Ravin v. State*,[94] the court recognized the fundamental right to privacy in one's home. In reviewing a state statute that prohibited the possession of marijuana by an adult for personal use in the home, the court inquired whether the statute was designed to accomplish a legitimate governmental interest and whether the means chosen bore a close and substantial relationship to that interest.[95]

After an extensive review of the available scientific evidence,[96] the court found that the potential harm was not great ***19** enough to show a close and substantial relationship between the state's interest in public welfare and marijuana use in the home.[97] However, the court did not find constitutional protection for the buying or selling of marijuana, the use of marijuana in a public place, or the possession of a large amount of marijuana at home.[98] Furthermore, the court did not hold that the possession or ingestion of marijuana was a fundamental right itself; rather, the court found that the privacy of one's home afforded protection from this type of governmental intrusion.[99]

In his concurring opinion in *Ravin*, Justice Boochever noted that federal privacy law was particularly unsettled and, citing *Baker v. City of Fairbanks*,[100] argued that it was therefore appropriate for the court to use independence and initiative in interpreting the privacy provision of the state constitution.[101] He also urged a broader interpretation than that found under the United States Constitution because, unlike the United States Constitution, "the citizens of Alaska, with their emphasis on individual liberty, enacted an amendment to the Alaska Constitution expressly providing for a right to privacy not found in the United States Constitution."[102] To achieve such broad protection, Justice ***20** Boochever argued for the use of "a single flexible test,"[103] which was, in reality, a sliding-scale analysis.

A follow-up case to *Ravin* was decided by the Alaska Supreme Court in 1978. In *State v. Erickson*,[104] the court ruled on whether the ingestion of cocaine in the home was protected by the right to privacy. The court's approach was substantially similar to the sliding-scale test used to address equal protection issues.[105] The test balances the infringing governmental conduct with the privacy interest in question. In Erickson, the privacy interest was similar to the one previously addressed in Ravin because it involved the use of illicit drugs in the defendant's own

home.[106] In Erickson, however, the drug in question was cocaine rather than marijuana. The court found the dangers presented by cocaine to exceed those posed by marijuana use.[107] Accordingly, the drug user's privacy interest was outweighed by the societal need to regulate the demonstrated dangers of cocaine.[108]

In the area of informational privacy, the Alaska Supreme Court has also employed a balancing test that appears to be yet another form of the sliding-scale standard. For example, in the 1977 case of *Falcon v. Alaska Public Offices Commission*,[109] a doctor challenged the requirement that he, as a member of a school board, had to release a list of the names of his patients to the commission. The court found that, while the doctor did not have a personal privacy stake in the list, the patients did.[110] The court balanced the state's interest in promoting fair and honest government ***21** with the patients' interest in concealing their identity and held that, until the state's means to its valid purpose provided some form of screening, the regulation must be suspended.[111] Moreover, in more recent cases involving information and privacy, the court has cited the Falcon balancing approach in applying a "compelling interest" test. The test applied in these privacy cases, however, is not the old two-prong test, but rather reflects a balancing approach as used in Falcon.[112]

Privacy law in Alaska is still developing. With respect to privacy in the home, a balancing or sliding-scale type of test is fairly well established. Nevertheless, in areas such as informational privacy, the court appears to be working to develop a balancing analysis.[113] Alaska's discourse on the right to privacy reflects both the state's independence and its unique tradition of emphasizing individual liberties. Alaska's discourse concerning privacy ***22** rights has involved not only an examination of the right itself but also the development of the test for judicial evaluation of the right. In cultivating this discourse, Alaska exemplifies the essence of NJF as well as the benefits of departing from the federal path.

Nelson, *supra, at* 17-22

. . . .

82
For a ten-year perspective on the development of the right to privacy in Alaska, see John F. Grossbauer, Note, *Alaska's Right to Privacy Ten Years After Ravin v. State* : Developing a Jurisprudence of Privacy, 2 Alaska L. Rev. 159 (1985).
83
See, e.g., *Griswold v. Connecticut*, 381 U.S. 479, 484 (1985).
84
501 P.2d 159 (Alaska 1972).
85
Id. at 166.
86
Id. at 166-67; see Alaska Const. art. I, s 1, set forth in the Appendix.
87
Breese, 501 P.2d at 174.
88
Id. at 169.

89
Id. at 174.
90
See, e.g., id. at 166 n.26.
91
458 P.2d 340 (Alaska 1969).
92
471 P.2d 386 (Alaska 1970).
93
See *Breese*, 501 P.2d at 166-67.
94
537 P.2d 494 (Alaska 1975).
95
Id. at 504.
96
As part of its analysis, the court considered evidence, including the state's justifications that marijuana is a psychoactive drug, it is harmful, heavy use entails a concomitant risk, it is capable of precipitating a psychotic reaction in at least some circumstances and its use adversely affects the user's ability to operate an automobile. Id. at 504-11.
97
Id. at 511.
98
Id.
99
Id. at 504. In 1990, Alaskans approved an initiative for a new statute recriminalizing the possession of marijuana in a private location. The 1990 Elections: State by State, N.Y. Times , Nov. 8, 1990, at B9. The resultant statute, see Alaska Stat. s 11.71.060 (Supp. 1994), while not yet before the state supreme court, would probably survive a constitutional challenge on the same grounds as the cocaine regulation in *Erickson*. New evidence as to the dangers of marijuana produced during the initiative drive has changed the balance from that present in 1975, when *Ravin* was decided.

Interestingly, Professor Gardner cites the *Ravin* case and the subsequent 1990 initiative for the proposition that "the Alaskan character for rugged individuality did not hold out for long against the nationwide hardening in attitudes against drug use." Gardner, supra note 2, at 828 n. 283. Perhaps if Gardner had examined the constitutional development surrounding this issue, he might have seen the case and initiative as part of a lively constitutional discourse rather than a sign of Alaskans' lost individuality.
100
471 P.2d 386 (Alaska 1970).
101
See *Ravin*, 537 P.2d at 513 (Boochever, J., concurring).
102
Id. at 514-15. The *Ravin* majority also noted the unique lifestyle in Alaska:
Our territory and now state has traditionally been the home of people who prize their individuality and who have chosen to settle or continue to live here in order to achieve a measure

of control over their own lifestyles which is now virtually unattainable in many of our other sister states.

Id. at 504 (majority opinion).

103

Id. at 515 (Boochever, J., concurring).

104

574 P.2d 1 (Alaska 1978).

105

See supra part IV.A.

106

See *Erickson*, 574 P.2d at 21.

107

Id. at 21-22.

108

While the discourse regarding the standards for equal protection and privacy claims has been complicated by cases raising both issues, the standards that have emerged are very similar, that is, a balancing test in both instances. The standard for equal protection claims as articulated in *Alaska Pacific Assurance Co. v. Brown*, 687 P.2d 264, 269-70 (Alaska 1984), is the substantial equivalent of the privacy test laid out in *Erickson*, namely, "[w] here the right to privacy is manifested in terms of interests more squarely within personal autonomy, the balance requires a heavier burden on the State to sustain the legislation in light of the right involved." *Erickson*, 574 P.2d at 22 n.144.

109

570 P.2d 469 (Alaska 1977).

110

See id. at 478-79.

111

Id. at 480.

112

See *Messerli v. State*, 626 P.2d 81 (Alaska 1980) (challenging campaign disclosure law on privacy, free speech and free press grounds). With this combination of rights, the *Messerli* court applied a strict compelling interest standard on the state's interest in general. The court held that the disclosures could be required only if adequate procedural safeguards were established. In discussing privacy, the court cited *Breese* for the proposition that the right to privacy is not absolute. Id. at 84. Given the combination of rights involved, *Messerli* can be viewed to illustrate balancing at the upper end or compelling interest level of review. The case also illustrates several areas where the Alaska constitution provides broader protections than the United States Constitution. Id. at 83.

State v. Oliver, 636 P.2d 1156 (Alaska 1981) also illustrates the court's application of a compelling interest test by balancing the privacy interests of a tax protestor claiming that a state requirement for the filing of a W-2 form violated the state right to privacy. The *Oliver* court noted that the information was neither highly sensitive nor intended to be kept confidential, and the court therefore concluded that the state's interest outweighed the protestor's. Id. at 1167-68. The court used language similar to that found in Falcon regarding the balancing of interests. Id. at 1167.

Nelson, *supra* at 41

UAS Privacy Considerations

Unmanned Aircraft Systems (UAS) are emerging technologies that have the potential to transform America by providing wide ranging economic, environmental, safety, and security benefits. A recent study[i] by the Association for Unmanned Vehicle Systems International conservatively estimates that 103,776 high paying jobs could be created and state tax revenue could exceed $482 million by 2025. They believe that every year the integration of UAS into the aviation system[ii] is delayed, America will lose more than $10 billion in potential economic impact.

UAS applications and benefits include assisting these civil government and commercial tasks: emergency deployment at accident scenes, search and rescue, barricade situations, structure or other fire emergencies, terror threats, firefighting, chemical and HAZMAT detection, crop dusting, agricultural development, monitoring of pollution, pipelines, wildlife, traffic, and floods, aerial news coverage, delivering medical supplies to remote areas, aerial photography, forensic photography, real-estate photography, filmmaking, communications, broadcasting, Arctic and volcanic research, damage assessment, cargo transportation, port, border, and event security, etc. In addition to these direct benefits, UAS implementation has the potential to spawn many new industries and provide an incredible array of manufacturing, operation, and other high paying job opportunities.

Along with these benefits come concerns about individual privacy. There is an existing body of federal, state and local law relating to privacy. The question is whether existing law is adequate, absent extensive judicial review, to alleviate the concerns of state legislators and citizens regarding privacy rights in light of this new technology. Because this technology can use a variety of sensors and some can potentially loiter for long periods of time without detection, there is a concern that government can use these systems to monitor individuals in a way that was not imagined in Supreme Court 4th Amendment rulings based on the presumption of privacy[iii]. Because state law interacts with Federal 4th Amendment rulings, states may choose to enact legislation addressing this issue. The challenge is to provide privacy protection while allowing the use of UAS to achieve UAS' many benefits, as described above.

Because of the complexity of this issue and the importance of privacy to citizens in every state, representatives of the Aerospace States Association (ASA)[iv], the Council of State Governments (CSG)[v], and the National Conference of State Legislatures (NCSL)[vi], have joined together to create considerations for states to evaluate in developing UAS legislation. As part of our impartial deliberative process, UAS privacy stakeholder associations including the ACLU, EPIC, and IACP Aviation Committee [vii], AUVSI – the industry trade association[viii] – as well as academics[ix] responded to our request to submit their suggestions for state privacy legislation to an independent law firm, Cadwalader, Wickersham & Taft LLP[x]. These submissions can be seen at http://aerostates.org/events/uas-privacy-submissions. Our review also included the Congressional Research Service's report, "Integration of Drones into Domestic Airspace: Selected Legal Issues," from April 4, 2013, and a memorandum for the Secretary from the Office of Civil Rights and Civil Liberties, U.S. Department of Homeland Security, dated September 14, 2012. After deliberation, ASA, CSG, and NCSL provide the following considerations:

1. Warrants: States may consider requiring a warrant for government surveillance of an individual or their property where the individual is specifically targeted for surveillance in advance without their permission. All other observation activities should not require a warrant, to the extent allowed under Supreme Court rulings. Additionally, if there is not a specific person identified for surveillance in advance, it is generally not possible to obtain a warrant. Requiring one would eliminate UAS benefits, but can be addressed per recommendation number two, below.

2. Data Concerns: Some are worried about government use of data derived from warrantless observations. States may consider addressing this by prohibiting the repurposing of data collected from Government use of UAS in warrantless observation unless a warrant allows the repurposing.

3. States may consider prohibiting commercial UAS and model aircraft flights from tracking specific, identifiable individuals without their consent.

4. States can consider prohibiting weapons to be carried by any UAS in commercial airspace.

5. States may consider endorsing the International Association of Chiefs of Police Aviation Committee (IACP) "Recommended Guidelines for the use of Unmanned Aircraft[xi]." These guidelines define UAS and provide guidance for community engagement, system requirements, operational procedures, and image retention for UAS operations by law enforcement organizations.

6. States may consider emphasizing that the FAA regulates commercial UAS[xii], and that they and model aircraft operations should be operated in a manner not to present a nuisance to people or property.

End Notes

[i] Economic Impact of Unmanned Aircraft Systems in the United States, March 2013, http://www.auvsi.org/econreport

[ii] The Federal Aviation Administration regulates all civil airspace, vehicles, and operators within the U.S. for safety and efficient airspace use through federal preemption. UAS safety regulations are being developed by the FAA. Until such regulations are in place, civil UAS operations must be specifically approved by the FAA. Government operations must comply with civil air traffic control directives. A lack of FAA permissive regulation and state prohibitions of UAS use delay integration of UAS into the aviation system and adversely affect America's global competitiveness in the development of this industry.

[iii] The crucial inquiry for Fourth Amendment protection is whether a person has a reasonable expectation of privacy that society is prepared to recognize. Courts have found that individuals may have a Fourth Amendment right against the unreasonable search and seizure of the area surrounding a house, referred to as the "curtilage." The Supreme Court has found that aerial surveillance over private property does not violate the Fourth Amendment if conducted by an aircraft in legally navigable airspace.

However, UAV's can fly lower, often undetected, and this holding might not apply to UAVs and their unique capabilities, and arguably remains an open question.

[iv] ASA is a bipartisan organization that represents the grassroots of American aerospace. It is a 501(c)(3) scientific and educational organization of lieutenant governors, governor-appointed delegates, and associate members from industry and academia. ASA was formed to promote a state-based perspective in federal aerospace policy development and to support education outreach and economic development opportunities.

[v] Founded in 1933, The Council of State Governments is our nation's only organization serving all three branches of state government. CSG is a region-based forum that fosters the exchange of insights and ideas to help state officials shape public policy. This offers unparalleled regional, national and international opportunities to network, develop leaders, collaborate and create problem-solving partnerships.

[vi] The National Conference of State Legislatures is a bipartisan organization that serves the legislators and staffs of the nation's 50 states, its commonwealths and territories. NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues. NCSL is an effective and respected advocate for the interests of state governments before Congress and federal agencies.

[vii] In response to our request for information, papers were received from the Airborne Law Enforcement Association (including and referencing the guidelines from the International Association of Chiefs of Police Aviation Committee), the American Civil Liberties Union, the American Legislative Exchange Council, the Electronic Frontier Foundation, the Electronic Privacy Information Center and the National Association of Criminal Defense Lawyers.

[viii] The Association for Unmanned Vehicle Systems International is the world's largest non-profit organization devoted exclusively to advancing the unmanned systems and robotics community. Serving more than 7,500 members from government organizations, industry and academia, AUVSI is committed to fostering, developing, and promoting unmanned systems and robotic technologies. AUVSI members support defense, civil and commercial sectors.

[ix] Douglas Marshall of New Mexico State University and Paul Voss of Smith College responded to our requests.

[x] Cadwalader, Wickersham & Taft LLP, established in 1792, is one of the world's leading international law firms, with offices in New York, Washington, D.C., Charlotte, Houston, London, Hong Kong, Beijing and Brussels. Cadwalader has provided pro bono legal services to ASA for over 20 years.

[xi] http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf

[xii] Code of Federal Regulations Title14, as amended.

The Aerospace States Association
107 S. West Street, Suite 510, Alexandria, VA 22314
Tel: (202) 257-4872 E-mail: AerospaceStates@comcast.net

May 3, 2013

Ms. Allie Bohm, American Civil Liberties Union

Dear Allie,

I am writing to invite you to join with the Aerospace States Association (ASA), the Council of State Governments (CSG), and the National Conference of State Legislatures (NCSL) in an important and timely dialogue on privacy issues related to incorporating Unmanned Aircraft Systems (UAS) into the national airspace.

I believe we all view privacy as a serious issue that our constituents are concerned about, yet we also see the long-term benefits in the use of unmanned aircraft for carrying out missions that are otherwise dirty, dull or dangerous. Commercial use could also create high paying jobs and environmental benefits that could transform our economy.

Many states have begun drafting legislation to address the privacy concerns related to UAS. We want to give thorough, thougtful consideration to all sides of the issues in order to develop suggested legislation for consideration by the states.

Please be a part of this effort by reviewing the attached plan we've developed and **submitting your comments to Bob Davis by Email to bob.davis@cwt.com, fax to 202-862-2400 or mailed by post to Cadwalader, 700 6th Street, NW, Suite 300, Washington, DC 20001 by June 1.** Your submission should address civil, commercial and personal use of UAS and contain your views on the "assumption of privacy" in UAS use. Your submission should not exceed three pages. An independent law firm, Cadwalader, Wickersham & Taft LLP, and leaders of state government associations will review your submission and draft best practices and suggested legislation based on your comments, to be presented at a roundtable discussion in Washington, D.C. on August 14. You are invited to participate in the roundtable to personally discuss the results of our drafting effort.

Thank you for your leadership, and for taking the time to participate in this dialogue.

Sincerely,

Mead Treadwell
Lieutenant Governor, State of Alaska
Chair, Aerospace States Association

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

May 30, 2013

Bob Davis
Cadwalader
700 6th Street, NW, Suite 300
Washington, DC 20001

Dear Mr. Davis:

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with more than a half million members, countless additional activists and supporters, and fifty-three affiliates nationwide, we appreciate the opportunity to comment on the privacy and civil liberties implications of domestic use of unmanned aircraft systems (UAS), also known as drones, and to recommend new protections for use of the technology.

Like any powerful surveillance tool, UAS have the potential to be used for good or ill. With implementation of good privacy ground rules, we can enjoy the benefits of this technology without bringing our country closer to a "surveillance society" in which every move is monitored, tracked, recorded, and scrutinized by the authorities.

UAS share some characteristics with manned aerial surveillance, such as planes and helicopters, but their threat to privacy is substantially greater in both scope and volume. Manned aircraft are expensive to purchase, operate, and maintain. They require trained pilots and ground crews and must land in order for pilots to rest. The expense both in dollars and in staffing has always imposed a natural limit on the government's aerial surveillance capacity. UAS's low cost and flexibility erode that natural limit. As technology improves, small, hovering devices will be able to explore hidden spaces, peer in windows, or even, potentially, enter homes, and large static blimps will enable continuous, long-term monitoring – all for much less than the cost of a helicopter or plane.

In our society, it is a core principle that the government does not collect information about individuals' innocent activities just in case they do something wrong. But UAS threaten to turn that principle on its head. What would be the effect on our society if everyone felt the keen eye of the government at all times? Psychologists have repeatedly found that people who are being observed tend to behave differently than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior."[1] There is a real danger that, if faced with the prospect of unregulated UAS, people will change how they behave in public – whether at a political rally or in their own backyards.

[1] Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," Scientific American, May 3, 2011, online at http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person; M. Ryan Calo, "People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship," 114 Penn St. L. Rev. 809, online at http://www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf.

UAS may also suffer from the problems we've seen with video surveillance – voyeurism,[2] racial profiling by operators,[3] and automated law enforcement.[4]

The Supreme Court has not yet had occasion to consider whether the Fourth Amendment places limits on government use of UAS. However, it has allowed some warrantless aerial surveillance from *manned* aircraft. Most notably, in the 1986 decision *California v. Ciraolo*, the Court ruled that there was no intrusion into Ciraolo's privacy when police borrowed an airplane, flew it over his backyard and spotted marijuana plants growing there, because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[5]

Nonetheless, because of their potential for pervasive use and their capacity for revealing far more than the naked eye, there are good reasons to believe that UAS may implicate Fourth Amendment rights in ways that manned flights do not. In both *Dow Chemical Co. v. United States*[6] and *Kyllo v. United States*,[7] the Supreme Court suggested that using sophisticated technology not generally available to the public may be considered a search under the Fourth Amendment.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

Further, the Supreme Court has suggested that the continuous use of a surveillance technology may heighten Fourth Amendment concerns. In *United States v. Knotts*, although the Court concluded that the use of the beeper in that case did not violate the Fourth Amendment, it held that if "such dragnet type law enforcement practices" as "twenty-four hour surveillance of any citizen of this country" ever arose, it would determine if different constitutional principles would be applicable.[8] Similarly, in *United States v. Jones*, five justices agreed (in two concurrences) that when the government engages in prolonged location tracking, it conducts a search under the Fourth Amendment.[9] While this decision may eventually play a role in regulating drone usage, the technology is moving far more rapidly than our jurisprudence, and it is critical that state legislatures act to protect their constituents' privacy.

State legislation should reflect the following key principles:

First, no one should be spied upon unless the government believes that person has committed a crime. Drone use over private property should occur only with a search warrant based on probable cause – the same standard used to search someone's house or business. It might be permissible to monitor individuals in public at a lower standard – perhaps reasonable suspicion – but the key is to prevent mass, suspicionless searches of

---

[2] "Did NYPD Cameras Invade A Couple's Privacy?" WCBS-TV report, Feb. 24, 2005, video no longer available online; Jim Dwyer, "Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop," *New York Times*, Dec. 22, 2005, online at http://www.nytimes.com/2005/12/22/nyregion/22rooftop.html.
[3] Clive Norris and Gary Armstrong, "The Unforgiving Eye: CCTV Surveillance in Public Spaces," Centre for Criminology and Criminal Justice at Hull University, 1997.
[4] Danielle Keats Citron, "Technological Due Process," 85 Washington University Law Review 1249 (2008), online at http://lawreview.wustl.edu/inprint/85/6/Citron.pdf.
[5] 476 U.S. 207 (1986).
[6] 476 U.S. 227 (1986).
[7] 533 U.S. 27 (2001).
[8] 460 U.S. 276, 283-84 (1983).
[9] 132 S. Ct. at 964 (Alito, J., concurring in judgment), 955 (Sotomayor, J., concurring).

the general population, including for intelligence gathering. Exceptions to this rule should be limited to emergencies connected to life and safety or narrowly drawn administrative exceptions in order to prevent pretextual use of drones.

Additionally, while the Constitution may permit UAS surveillance of public spaces on less than a probable cause standard, the vast majority of the 96 different drone bills being considered in 43 states this legislative session[10] require law enforcement to get a probable cause warrant before using a drone in an investigation, whether that investigation occurs in private or public space, a good indicator that a warrant requirement for drone use is both workable and palatable. Already, warrant requirements have been enacted in Florida,[11] Idaho,[12] Montana,[13] and Tennessee.[14]

Second, images of identifiable individuals captured by law enforcement UAS should not be retained or shared unless they are of the target of the investigation that justified drone deployment, and there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

Third, while drone use should be permitted for reasonable non-law enforcement purposes where privacy will not be substantially affected, such as geological inspections or environmental surveys, information collected by drones for one purpose should not be used for another purpose such as general law enforcement or enforcing administrative laws.

Fourth, drones should not carry weapons.

Finally, oversight is crucial. Communities must play a central role in deciding whether to purchase drones, and the policies and procedures for the use of UAS should be explicit and written, and should be subject to public review and comment. Similarly, like any new technology, drone use must be monitored to make sure it's a wise investment that works.

Placing reasonable limitations on law enforcement is by no means a new idea – for example, authorities may take a thermal image of someone's home only when they get a warrant – and it is imperative that we implement a system of rules to ensure that we can take advantage of UAS technology without sacrificing our privacy. If you have any questions, would like to discuss the issue further, or would like to see ACLU's model state legislation, please don't hesitate to reach out to me at abohm@aclu.org or (212) 284-7335.

Sincerely,

Allison S. Bohm, Advocacy & Policy Strategist

---

[10] "States with UAS Legislation" National Conference of State Legislatures. May 29, 2013. http://www.ncsl.org/issues-research/justice/unmanned-aerial-vehicles.aspx.
[11] S.B. 92 (Fla. 2013)
[12] S.B. 1134, 62nd Legislature (Idaho 2013)
[13] S.B. 196, 63rd Legislature (Mont. 2013)
[14] S.B. 796 (Tenn. 2013)

MEMORANDUM

State of Alaska
Department of Law

TO: Mead Treadwell
Lieutenant Governor
State of Alaska

FROM: Libby Bakalar
Assistant Attorney General
Transportation Section

CC: Jim Cantor
Deputy Attorney General
Department of Law

Margie Vandor
Chief Assistant Attorney General
Department of Law

Michaela Goertzen
Speechwriter
Office of the Lieutenant Governor

DATE: May 20, 2013

FILE NO.: JU2011200514

TEL. NO.: 907.465.3600 main
907.465.2520 fax

SUBJECT: Legal issues related to unmanned aircraft systems

I. Introduction and background.

In your capacity as chair of the Aerospace States Association, you asked me to provide you with a brief description and analysis of the core legal issues related to the civilian use of Unmanned Aircraft Systems (UAS), also known as "drones." The context for your inquiry is the University of Alaska's pending application with the Federal Aviation Administration (FAA) to become one of a limited number of testing sites in the nation for UAS. Please note that this document is not legal opinion of the Office of the Attorney General, but rather simply a compendium of my research and a preliminary analysis.

UAS are unmanned aircraft designed to do tasks that are too difficult, dull, dangerous, or expensive for manned aviation, and are designed to carry a "system payload" such as a camera or sensor.[1] Traditionally, UAS have been used for military

[1] Association for Unmanned Vehicle Systems International ("AUVSI"), UAS Privacy Issues Document.

purposes, but they are being increasingly deployed in domestic civilian contexts such as law enforcement, disaster relief, fire-fighting, agriculture, energy, industry, wildlife tracking, and others.[2] Commercial use of UAS is currently prohibited, but that is expected to change by 2014.[3] UAS can range in size from smaller than a cell phone to larger than a commercial jetliner.[4] Research sponsored by the Association for Unmanned Vehicle Systems International (AUVSI), a non-profit trade association that supports the civilian use of UAS, concluded that the integration of UAS into the national airspace has the potential to create more than 100,000 new jobs and $82 billion of economic impact by 2025.[5]

The legal issues surrounding the civilian use of UAS relate mainly to privacy and property interests, and are relatively untested in the courts because of the novelty of the technology involved and the regulatory vacuum in which that technology operates. Fortunately, there has been significant legal scholarship as well as congressional reporting[6] in in this area, all of which I rely upon heavily in this memorandum. I have also reviewed all the materials Charles Huettner emailed me after our April 5th teleconference. Some limited case law also exists on the privacy concerns raised by aerial surveillance and similar technologies. These cases telegraph how the Supreme Court might view the privacy implications of UAS. Following is the requested description, summary, and analysis of the issues that have arisen and been analyzed by legal scholars to date. I also discuss the Alaska-specific implications of these issues, which are not discussed in any of the law reviews, journals, or reports.

II. Core legal issues raised by the use of UAS/drones.

The FAA oversees all aircraft operations in the United States and makes and

---

2 *See* Villasenor, John, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J.L. & Pub. Pol'y 458, 459 (2013).

3 *Id.* at 471.

4 *Id.* at 465.

5 "The Economic Impact of Unmanned Aircraft Systems Integration in the United States," AUVSI, March, 2013.

6 *See* Integration of Drones into Domestic Airspace: Selected Legal Issues, Congressional Research Service, CRS Report for Congress (April 4, 2013).

enforces rules to implement and interpret laws passed by Congress governing aviation.[7] Federal law enacted in February 2012 (The Federal Aviation Administration Modernization and Reform Act of 2012) requires the FAA to devise a comprehensive plan to integrate all civilian UAS into the national airspace system by September 30, 2015, appropriates billions of dollars in funding, and creates the six UAS test sites for which many states, including Alaska, are vying.[8]

The federal government is still struggling with the regulation of UAS, specifically, how to define these vehicles, how to clarify which—if any—existing regulations apply to them, how to craft future regulations to encompass vehicles not governed by existing regulations, and how to ensure that future regulations do not inadvertently regulate other industries such as model or hobby aircraft.[9] The FAA will need to identify technology (*e.g.* cameras and radar) that will obviate the need for regulations requiring pilots to "see and avoid" other aircraft, address appropriate training for UAS operators, devise proper procedures for when a UAS loses contact with an operator or is hacked, coordinate with other countries and agencies in adopting regulations, and ensure that there is sufficient wireless spectrum to accommodate the communication needs of these vehicles.[10] Presently, UAS operators engaged in both public aircraft operations and private operations are required to have special certifications from the FAA.[11]

There is no legislation yet governing UAS in Alaska, although there is model legislation that AUVSI is compiling, and according to news reports, at least one other state—Florida—has begun to legislate UAS. Two bills were introduced in Alaska last session that touch upon UAS: HB 159, "An Act relating to the admissibility of evidence acquired through the use of an unmanned aerial vehicle; establishing a crime for certain uses of unmanned aerial vehicles; and restricting the use of unmanned aerial vehicles for collection of information or investigation by peace officers and other government agents;" and HCR 6, "Recognizing the Alaska Center for Unmanned Aircraft Systems

---

7 Villasenor, *supra* note 2, at 469.

8 P.L. No. 112-095 (Feb. 14, 2012).

9 *See* Kapnik, Benjamin, *Unmanned but Accelerating: Navigating the Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System*, 77 J. Air L. & Com. 439, 443 (2012).

10 *Id.* at 448-49.

11 Villasenor, *supra* note 2, at 471.

Integration at the University of Alaska Fairbanks as a national leader in unmanned aircraft research and development; and relating to a Task Force on Unmanned Aircraft Systems." Presumably, these bills could be revisited next session.

Any discussion of UAS legislation must also consider federal pre-emption and the interplay between state and federal law. Although aircraft safety, trade, and noise regulation is the established provenance of the federal government, states may still pass laws governing how aircraft are flown.[12] Both Alaska and federal law prohibit the reckless operation of aircraft, but Alaska could not enact privacy laws that would decrease or implicate in any way the safety of flight operations, such as laws governing aircraft speed or altitude.[13] From a pre-emption standpoint, the safest area for state legislation is in the realm of privacy laws aimed at non-government actors that address trespass, invasion of privacy, stalking, and harassment, because state power to legislate in this area is well-established.[14]

In short, there is both a mandate and pressing need to legislate and regulate UAS at both the state and federal level. However, the precise parameters and scope of that legislation and regulation remain nebulous at best.

III. Constitutional rights.

A. The Fourth Amendment.

Probably the biggest legal issue surrounding UAS is the implications of these devices for individual privacy rights. The Fourth Amendment to the United States Constitution guarantees to the people the right to be free from unreasonable search and seizure by the government.[15] The Alaska Constitution contains an analogous search and seizure provision, as well as an explicit clause guaranteeing to its citizens the right to privacy.[16] Because the FAA is primarily a regulating agency whose mandate is to ensure

---

12 Villasenor, *supra* note 2, at 513.

13 *Id.*

14 *Id.*

15 *See* U.S. Const. amdt. IV.

16 Alaska Const. art. I, §§ 14 and 22. Note that these provisions bind only government actors—not private citizens.

the efficient and safe operation of U.S. airspace, questions have arisen whether this agency is really the appropriate entity to ensure that government actors using UAS are not violating these basic constitutional principles or whether constitutional privacy compliance should be spearheaded at the state or federal level by some other agency. It is clear, however, that no government actor may commit such violations.

The crucial inquiry for Fourth Amendment and state constitutional privacy purposes is whether a person has a reasonable expectation of privacy that society is prepared to recognize. One scholar notes that "[w]here a [UAS] captures images that could have been obtained from civilian aircraft traveling in a legally authorized manner, privacy claims are limited. Consumers lack a reasonable expectation of privacy with respect to areas already exposed to civilian over-flights."[17] However, novel imaging technologies such as thermal and infrared imaging could raise concerns. Indeed, as noted by another scholar who has examined the issue, "[t]he privacy issues raised by the potential ubiquity of [UAS] go beyond the current Fourth Amendment jurisprudence."[18] Indeed, "[t]here is no precedent that squarely addresses privacy implications of governmental use of a technology that allows essentially permanent, multi-dimensional, multi-sensory surveillance of citizens twenty-four hours a day."[19]

However, there has been some judicial guidance. *Katz v. U.S.*[20] was a landmark Fourth Amendment case in which the Supreme Court held for the first time that a Fourth Amendment violation could occur absent a physical intrusion—specifically, through a listening device the police had affixed to the outside of a public phone booth. This was the first "remote sensing" case, soon to be followed by a trilogy of key "aerial surveillance cases."

The "remote sensing" cases fall into two categories: "open fields" and "curtilage." Remote sensing in "open fields" does not implicate the Fourth Amendment because open

---

17 Geoffrey Christopher Rapp, *Unmanned Aerial Exposure: Civil Liability Concerns Arising from Domestic Law Enforcement Employment of Unmanned Aerial Systems*, 85 N.D.L. Rev. 623, 641 (2009).

18 Joseph J. Vacek, *Big Brother Will Soon Be Watching—Or Will He?*, 85 N.D. L. Rev. 673, 674 (2009).

19 *Id.* at 675.

20 389 U.S. 347 (1967).

fields are areas of public and private property that "do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government surveillance or interference."[21] However, "curtilage" is a legal "penumbra" surrounding a home where the Fourth Amendment may be implicated.[22] Whether a given area constitutes "curtilage" depends on the proximity of the area to the home, whether the area is enclosed, the nature of the use to which the area is put, and the steps taken by the resident to protect the area from observation.[23] Although a person may have reasonable expectations of privacy in curtilage, remote sensing of curtilage "does not require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[24] The bottom line is that remote sensing will not implicate the Fourth Amendment "if it is done from a public vantage point where law enforcement officers can make open observations."[25]

The Supreme Court's "aerial surveillance" trilogy consists of *California v. Ciraolo*,[26] *Florida v. Riley*,[27] and *Dow Chemical Company v. U.S.*[28] All three cases were decided in the 1980s. Together, they stand for the proposition that aerial surveillance of any kind over private or commercial property from aircraft that are lawfully in navigable airspace is not a Fourth Amendment search, because there is no reasonable expectation of privacy in an area that is openly visible from above, regardless whether the area is curtilage or an open field.[29]

---

21 *Oliver v. U.S.*, 466 U.S. 170, 179 (1984).

22 *U.S. v. Dunn*, 480 U.S. 294, 300 (1987).

23 *Id.* at 301.

24 *California v. Ciraolo*, 476 U.S. 207, 213 (1986).

25 Vacek, *supra* note 18, at 680.

26 476 U.S. 207 (1986).

27 488 U.S. 445 (1989).

28 476 U.S. 227 (1986).

29 Vacek, *supra* note 18, at 682.

In *Ciraolo*, police flew a fixed-wing aircraft 1,000 feet over a defendant's backyard, the minimum safe altitude required by FAA regulations, and observed marijuana plants with the naked eye. The backyard was not visible due to an extensive fencing system, so the aerial search provided the basis for a search warrant and marijuana plants were found after a physical search. The Court held that a ground fence does not create an expectation of privacy to be free from aerial searches because routine flights exposed the backyard to public view.[30]

Riley reached the same holding when officers flew a helicopter 400 feet overhead to peer through openings in a greenhouse and determined marijuana was growing inside the defendant's fenced-in home. Again, the Court found that there was no reasonable expectation of privacy because helicopter flight in navigable airspace was a routine, expected occurrence.[31]

And in *Dow Chemical*, the Environmental Protection Agency, acting without a warrant, hired a private commercial pilot to fly over Dow's property to take aerial photos of suspected regulatory violations. The Court upheld this conduct because "such an industrial complex is more comparable to an open field and as such it is open to the view and observation of persons in aircraft lawfully in the public airspace."[32]

However, decades later in 2001, in *Kyllo v. United States*,[33] the Supreme Court reminded us that the Fourth Amendment protects people—not just places—from unreasonable searches and seizures. *Kyllo* involved law enforcement's warrantless use of thermal imaging to detect unusual amounts of heat radiating from the defendant's home, indicating the presence of marijuana. *Kyllo* held that this surveillance violated the Fourth Amendment because the technology was not in widespread use. Currently, *Kyllo* limits the ability of law enforcement to rely on infrared/thermal imaging technology, but because the Court's decision was directly linked to the prevalence of the technology, it's an open question whether the Court's limitation would persist if these technologies went into more "widespread use." As one scholar put it, "the test seems to turn on whether

---

30 476 U.S. at 215.

31 488 U.S. at 450-51.

32 476 U.S. at 239.

33 553 U.S. 27 (2001).

Wal-Mart sells it or not."[34] Such a question would most likely be tested in a criminal context, where the prosecution seeks to admit evidence obtained through the use of these technologies.

Finally, just last year, in *United States v. Jones*,[35] the Supreme Court held that the installation of a GPS tracking device on a suspect's car for eight days constituted a search under the Fourth Amendment. Although *Jones* did not deal with aerial surveillance, the Court held that the placement of the device was a physical intrusion onto private property for the purposes of obtaining information, as well as the extended monitoring of a person in a public space, both of which constituted a Fourth Amendment "search." Some scholars have predicted that one potential result of *Jones* is that extended UAS surveillance could constitute a search within the meaning of the Fourth Amendment.[36]

It is clear from a review of the scholarship and the limited case law that the rate of advancement of these technologies often outpaces the ability of courts to rule upon the validity of their use under the Fourth Amendment. The overall conclusion so far is that aerial surveillance by any method, at a legal altitude, is constitutional if the technology is in general public use and does not trespass upon private property for extended periods of time. Still, the legal landscape has been characterized as "an aeronautical Wild West," and the current regulatory scheme as "inadequate to deal with the novel issues raised" by the use of UAS, particularly by law enforcement.[37]

In Alaska, we must consider an additional important factor: Article I, section 22 of the Alaska Constitution guarantees an explicit individual right to privacy. There is no state case law interpreting this clause (or any part of the state constitution) in the context of UAS. However, it is highly possible that the Alaska Supreme Court would interpret the right in favor of the individual asserting it as opposed to deferring to the government. For example, our Supreme Court has interpreted the privacy clause to create a constitutional right to privacy in garbage placed for collection, which contrasts with both state and

---

34 Vacek, *supra* note 18, at 683.

35 132 S. Ct. 945 (2012).

36 Kapnik, *supra* note 9, at 495.

37 Vacek, *supra* note 18, at 675-77.

federal case law on the Fourth Amendment.[38] The take-away point here is that government conduct that complies with the Fourth Amendment under either the state or federal constitution could *nonetheless* violate the state constitutional right to privacy. And in 2002, at least one member of the Alaska Court of Appeals, albeit in a concurring and unreported opinion, expressed constitutional skepticism at law enforcement's surreptitious use of infrared helicopter technology of the type prohibited under *Kyllo* the year before.[39]

B. The First Amendment & individual privacy.

In addition to the Fourth Amendment implications of government-operated UAS, these vehicles may also implicate the First Amendment rights of private citizens to collect and gather information. One scholar has recently addressed this issue, noting that for private entities and persons not bound by the Fourth Amendment, the key constitutional question is the extent of these persons' First Amendment right to access information.[40] The Supreme Court long ago held that the First Amendment protects the act of seeking out news, otherwise "freedom of the press could be eviscerated."[41] And at least one circuit court of appeals has recently held that the First Amendment permits a private citizen to record the actions of people in a public space.[42] Congress could potentially enact laws to protect individuals from intrusive UAS surveillance by private actors, which would be considered in a First Amendment context of the right to gather and receive information.[43] Such bills have been introduced, but none have yet been enacted.[44] Because the civilian use of UAS is nascent, and there is no controlling Supreme Court

---

38 *Cf. Beltz v. State*, 221 P.3d 328 (Alaska 2009) and *California v. Greenwood*, 486 U.S. 35 (1988).

39 *See Johnston v. State*, 2002 WL 563609 (April 17, 2002) (Mannheimer, J., concurring) (unpublished opinion).

40 Villasenor, *supra* note 2, at 498.

41 *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972).

42 *Glik v. Cunniffe*, 655 F.3d 78, 82 (1st Cir. 2011).

43 *See* Integration of Drones into Domestic Airspace: Selected Legal Issues, Congressional Research Service, CRS Report for Congress (April 4, 2013).

44 *Id.*

case law, it remains to be seen how far First Amendment protections will extend in this area.

The privacy rights of individuals and businesses exist in perpetual tension with the First Amendment rights of non-government actors to gather information, and that tension could give rise to actionable claims for privacy violations. Common law invasions of privacy could occur if UAS use "intrudes upon seclusion" in the home or results in the "publication of private facts," which are the two main categories of invasion of privacy claims. Intrusion upon seclusion occurs where the intrusion was intentional and would be highly offensive to a reasonable person.[45] A publication of private facts claim could arise where a UAS takes images of private individuals involuntarily caught up in newsworthy events, and those images conveyed facts not previously known to the public.[46] Similarly, the use of UAS could potentially give rise to criminal liability under both federal and state anti-stalking and harassment laws.[47] Finally, UAS could be used by private citizens to investigate or monitor potential health and safety violations by businesses, or engage in corporate espionage. Such conduct raises complex and unanswered questions about a private citizen's right to do under the First Amendment what the government could not do under the Fourth.

In short, the above concepts are nothing new to the First Amendment and privacy arena, but they must and will be revisited in light of UAS enhanced imaging capabilities, ease of use, and ever-increasing availability. As discussed in detail above, the strong privacy protections of the Alaska Constitution make it highly likely that individual privacy rights implicated by UAS will be more zealously legislated and enforced in Alaska than in other jurisdictions.

C. Property rights, & tort liability; nuisance, trespass, & ground damage.

Property owners could potentially file tort claims for nuisance and/or trespass against operators of UAS. According to a preeminent torts treatise, a trespass claim against an aircraft operator is viable only when the aircraft "enters into the immediate reaches of the air space next to the land" and "interferes substantially with . . . the use and

---

45 Restatement (Second) of Torts § 625B (1977).

46 Villasenor, *supra* note 2, at 503.

47 *Id.* at 505.

enjoyment" of the property by the landowner."[48] The navigable airspace regulated by the FAA is considered a public highway, but it appears that anywhere between 50 to 150 feet above the property owner could be considered impermissible interference with private property.[49] Accordingly, UAS that operate within this window of airspace could potentially raise trespass claims, and UAS that generate noise, light, pollution, or vibration could lead to viable nuisance claims by homeowners.[50] Additional tort claims could arise if a UAS caused ground damage to personal or real property.

Title 2 of the Alaska Statutes is devoted entirely to the regulation and operation of aircraft ("Aeronautics"). Alaska Statute 02.30.030 provides that "A person may not operate an aircraft in the air or on the ground or water in a careless or reckless manner so as to endanger the property of another." This statute directs the court, when evaluating such claims, to consider "the standards for safe operation of aircraft prescribed by federal statutes or regulations governing aeronautics." The phrase "operate aircraft" is defined in AS 02.30.050 as "to use, navigate, pilot, or taxi an aircraft in the airspace over this state, or upon the land or water inside the state." This chapter does not contain a definition of "aircraft." However, "aircraft" is defined in the general provisions of Title 2 (Alaska Aeronautics Act of 1949) as "a contrivance used or designed for navigation of flight in the air,"[51] which could be read to include UAS, although this definition was enacted prior to the burgeoning use of civilian UAS. Accordingly, I am uncertain whether UAS would fit into the current statutory definition of "aircraft," and therefore I think it's an open question whether a court would find that the foregoing provisions regarding liability for aircraft operation would automatically apply to operation of UAS or whether additional statutory language would be necessary to expand that definition. My instinct is that UAS should be specifically legislated in this manner.

If Alaska chooses to enter this arena by passing laws or regulations, it is advisable for the legislature to also enact a statutory immunity provision. That way, the state may

---

48 American Law Institute, Restatement (Second) of Torts § 159 (2009) cmt. i.

49 Rapp, *supra* note 17, at 645 (citing *id.*). See also *United States v. Causby*, 328 U.S. 256 (1946) (rejecting the common law concept that a homeowner owns all the airspace above his property up to the heavens, but rather owns "at least that much space above the ground as he can occupy or use in connection with the land.").

50 *Id.*

51 AS 02.15.260(2).

avoid liability for damages in tort when two private UAS collide and fragments cause damage to people or property. Such immunity clauses are common and can deflect an argument that the state is liable simply because it has chosen to legislate in a particular topic area.[52]

D. Environmental concerns.

Scholars have observed the potential of UAS to generate environmental concerns, which could be starker in Alaska than elsewhere. Alaska is already a hotbed of environmental litigation. Many UAS contain batteries, circuitry, and chemicals that could leach into the ground, and the flight of UAS and the noise they cause could disrupt birds and other wildlife habitats.[53] Environmental groups and private citizens could potentially raise federal claims regarding the operation of UAS under the National Environmental Policy Act, the Endangered Species Act, or the Noise Control Act.[54]

In Alaska, to the extent UAS and the execution of implementing statutes interfere with state fish, wildlife, and waters, the government could be found in violation of the "common use" and "sustained yield" provisions of the Alaska Constitution, which provide, respectively, that the state, fish, wildlife and waters of the state are reserved to the people for their common use and that replenishable resources belonging to the state must be utilized, developed, and maintained according to the sustained yield principle.[55]

E. Communications interference.

UAS also have the potential to interfere with existing civilian communications systems used to operate cell phones, satellite TV signals, and other wireless and telecommunications technology.[56] Further, signal loss between UAS and its ground

---

52 *See, e.g.*, AS 09.65.215 (Immunity of peace officer for use of body wire eavesdropping device); AS 09.65.235 (Immunity for negotiated regulation making committee and its members); AS 09.65.250 (Immunity for certain actions related to child support); AS 09.65.330 (Immunity: Use of defensive force).

53 Rapp, *supra* note 17, at 632.

54 *Id.*

55 Alaska Const. art. VIII, §§3, 4.

56 Rapp, *supra* note 17, at 640-41.

control operations could result in a mid-air collision or ground damage.[57] This problem could be somewhat mitigated by the assignation of UAS to specific frequencies once UAS are fully integrated into the national airspace, but the potential for interference still remains.[58]

Under state law, the Department of Transportation and Public Facilities is responsible for supervising, developing, and promoting "aeronautics and communications inside the state . . ."[59] The Department could be held responsible for ensuring, through properly adopted regulations and in conjunction with the federal government, that UAS do not unduly interfere with existing civilian communications systems in the state.

F. Mid-air collisions.

Finally, mid-air collisions of UAS with other aircraft and with each other are always a possibility. Most UAS lack the sophisticated collision avoidance systems required of many manned aircraft, and the absence of an on-board pilot who can physically observe other aircraft exacerbates the risk of a mid-air collision.[60] Furthermore, the "small size and radar profile of [UAS] create significant risk that such craft would damage civilian aircraft, causing both property loss and human casualties."[61]

As described above, individual citizens could file tort claims under state law for damages against operators of UAS or the government associated with such accidents. Collisions and near-collisions have already resulted from the use of UAS at the military level, and the scholarship predicts that "[i]t is hard to imagine widespread integration of [UAS] into populated airspace without some level of air-to-air accidents rising."[62]

---

57 *Id.*

58 *Id.*

59 AS 02.10.010(a)-(b).

60 Rapp, *supra* note 17, at 629; 640-41.

61 *Id.*

62 *Id.*

IV. Conclusion.

There are many more questions than answers surrounding the increased civilian use and operation of UAS, because there is no case law that definitively resolves any of the issues discussed above, and there is a regulatory vacuum. Indeed, "[t]he only certain aspect of the debate about unmanned aircraft and privacy is that it will be contentious."[63] However, identifying and analyzing these issues at the executive level is the first step to crafting legislation that attempts to address them. Only when those laws are tested in the courts will we fully come to understand the interplay between the technological advantages offered by UAS, the reach of constitutional protections, and the scope of actionable legal claims.

EMB/tjd

---

63 Villasenor, *supra* note 2, at 516.

AIRBORNE LAW ENFORCEMENT ASSOCIATION

50 Carroll Creek Way, Suite 260, Frederick, MD 21701
Bus (301) 631-2406 Fax (301) 631-2466 singley@alea.org
www.alea.org

June 5, 2013
Mr. Bob Davis
Cadwalader, Wickersham & Taft LLP
700 6th Street, NW, Suite 300
Washington, DC 20001

Dear Mr. Davis:

On behalf of the Airborne Law Enforcement Association (ALEA) and the International Association of Chiefs of Police (IACP) Aviation Committee, we are pleased to submit the following comments regarding the "Privacy Legislation Plan 2013."

To begin, our respective organizations support and promote the IACP Aviation Committee's *Recommended Guidelines for the use of Unmanned Aircraft* (see Exhibit A) and the Association for Unmanned Vehicle Systems International's (AUVSI) *Unmanned Aircraft System Operations Industry "Code of Conduct"* (see Exhibit B). We do not concur with privacy advocates who claim that public safety agencies' utilization of unmanned aerial systems (UAS) poses a greater threat to "privacy rights" than manned aviation. Similarly, we do not concur that said uses pose a greater threat to privacy "rights" than other technologies currently utilized by public safety agencies, both in manned aircraft and on the ground. Furthermore, we do not accept that any legislation is necessary as there are long-standing court rulings upholding our Fourth Amendment protections; but we are particularly opposed to legislation that focus their attention on one technology based on fears of what could occur tomorrow, however unlikely. Aside from recent laws enacted that place outright bans on UAS use, such as that in Charlottesville, VA, many current "anti-drone" bills appear to be more of an attempt to increase protections under the Fourth Amendment without actually altering the U.S. Constitution. The presumption in most of these pieces of legislation is that a reasonable expectation of privacy now exists in places where there has been no such expectation. As such, a warrant must be obtained before UAS can be utilized by public safety.

While U.S. Customs and Border Protection (CBP) has unique operational needs that require larger, longer flight duration aircraft, local, state, and other federal agencies, even if they could afford to acquire and operate similar systems, have no interest in utilizing these types of assets. What they are interested in obtaining are small unmanned aerial systems (sUAS) that are inexpensive, lightweight, portable, and quickly and easily deployable.

sUAS come in two forms: gas powered and battery powered. Within these categories, there are fixed-wing and rotory-wing models. Gas powered sUAS tend to be heavy, loud, and can fly for greater periods of time. Battery powered sUAS are lightweight, relatively quiet, slower, and have short flight durations, especially for the rotory-wing models.

As such, sUAS that are available to public safety, coupled with the Federal Aviation Administration's (FAA) regulations governing the use of UAS by public safety (e.g., cannot exceed 4.4 pounds, cannot exceed 400 feet above ground level (AGL), can only be operated during daylight conditions, and must remain within line of sight of the operator at all times), make this new technology a poor candidate for "spying," as well as for persistent surveillance operations. The fact of the matter is, "spying" and persistent surveillance can be done much more effectively by manned aircraft and ground personnel, than with any sUAS.

With that said, if legislation is to be drafted, we suggest that the following be considered:

1. The courts have determined in their interpretations of Fourth Amendment cases, that citizens have a "reasonable expectation of privacy." Be cognizant that changing the circumstances under which people have reasonable expectations of privacy can have unintended consequences. If a law enforcement agency determined that the use of a sUAS during a public event was necessary to maintain public safety (assuming that such use would even be permissible under FAA rules), but there is a law requiring that a warrant be issued prior to its use in that capacity, the sUAS could not be used because a judge would have no one to write a warrant for. At the same time, law enforcement conducts these operations regularly with manned aircraft. Why? Because the courts have already determined that there is no reasonable expectation of privacy in such a setting. Does it make sense to have a law that creates a different reasonable expectation of privacy for a UAS from anything else? Will we be seeing legislation developed then for cell phones? GPS? Video cameras? Having more than one "reasonable expectation of privacy" standard is unworkable in law enforcement.

2. Concentrate on sensitive data collection, use, distribution, storage, and purging of data and not on the technology that was used to obtain the data originally. If a person's "reasonable expectation of privacy" is violated by an "unreasonable search and seizure," the device used to create that violation, whether it's a global satellite positioning system, computer, cell phone, video pole camera, manned aircraft camera, unmanned aircraft camera, etc., is irrelevant.

3. Legislation needs to focus on the law enforcement agency utilizing sound policy to govern the use of sUAS technology. The policy should be in accordance with the IACP Guidelines; these Guidelines are a solid starting point for the development of policies for the use of sUAS.

We appreciate the opportunity to have input into this process and look forward to participating in the upcoming roundtable meeting in Washington, DC on August 14.

Sincerely,

Stephen J. Ingley
Executive Director
Airborne Law Enforcement Association

Don R. Roby
Captain
Baltimore County Police Department
Chair
IACP Aviation Committee

Cc: ALEA Board of Directors
IACP Aviation Committee

EXHIBIT A

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

AVIATION COMMITTEE

Recommended Guidelines for the use of Unmanned Aircraft

BACKGROUND:

Rapid advances in technology have led to the development and increased use of unmanned aircraft. That technology is now making its way into the hands of law enforcement officers nationwide.

We also live in a culture that is extremely sensitive to the idea of preventing unnecessary government intrusion into any facet of their lives. Personal rights are cherished and legally protected by the Constitution. Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety. From enhanced officer safety by exposing unseen dangers, to finding those most vulnerable who may have wandered away from their caregivers, the potential benefits are irrefutable. However, privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UA by their police.

The Aviation Committee has been involved in the development of unmanned aircraft policy and regulations for several years. The Committee recommends the following guidelines for use by any law enforcement agency contemplating the use of unmanned aircraft.

DEFINITIONS:

1. **Model Aircraft** - A remote controlled aircraft used by hobbyists, which is manufactured and operated for the purposes of sport, recreation and/or competition.
2. **Unmanned Aircraft (UA)** – An aircraft that is intended to navigate in the air without an on-board pilot. Also called Remote Piloted Aircraft and "drones."
3. **UAS Flight Crewmember** - A pilot, visual observer, payload operator or other person assigned duties for a UAS for the purpose of flight.
4. **Unmanned Aircraft Pilot** - A person exercising control over an unmanned aircraft during flight.

COMMUNITY ENGAGEMENT:

1. Law enforcement agencies desiring to use UA should first determine how they will use this technology, including the costs and benefits to be gained.
2. The agency should then engage their community early in the planning process, including their governing body and civil liberties advocates.
3. The agency should assure the community that it values the protections provided citizens by the U.S. Constitution. Further, the agency will operate the aircraft in full compliance with the mandates of the Constitution, federal, state and local law governing search and seizure.
4. The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy.
5. As with the community, the news media should be brought into the process early in its development.

SYSTEM REQUIREMENTS:

1. The UAS should have the ability to capture flight time by individual flight and cumulative over a period of time. The ability to reset the flight time counter should be restricted to a supervisor or administrator.
2. The aircraft itself should be painted in a high visibility paint scheme. This will facilitate line of sight control by the aircraft pilot and allow persons on the ground to monitor the location of the aircraft. This recommendation recognizes that in some cases where officer safety is a concern, such as high risk warrant service, high visibility may not be optimal. However, most situations of this type are conducted covertly and at night. Further, given the ability to observe a large area from an aerial vantage point, it may not be necessary to fly the aircraft directly over the target location.
3. Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program.

4. The use of model aircraft, modified with cameras, or other sensors, is discouraged due to concerns over reliability and safety.

OPERATIONAL PROCEDURES:

1. UA operations require a Certificate of Authorization (CAO) from the Federal Aviation Administration (FAA). A law enforcement agency contemplating the use of UA should contact the FAA early in the planning process to determine the requirements for obtaining a COA.
2. UAS will only be operated by personnel, both pilots and crew members, who have been trained and certified in the operation of the system. All agency personnel with UA responsibilities, including command officers, will be provided training in the policies and procedures governing their use.
3. All flights will be approved by a supervisor and must be for a legitimate public safety mission, training, or demonstration purposes.
4. All flights will be documented on a form designed for that purpose and all flight time shall be accounted for on the form. The reason for the flight and name of the supervisor approving will also be documented.
5. An authorized supervisor/administrator will audit flight documentation at regular intervals. The results of the audit will be documented. Any changes to the flight time counter will be documented.
6. Unauthorized use of a UA will result in strict accountability.
7. Except for those instances where officer safety could be jeopardized, the agency should consider using a "Reverse 911" telephone system to alert those living and working in the vicinity of aircraft operations (if such a system is available). If such a system is not available, the use of patrol car public address systems should be considered. This will not only provide a level of safety should the aircraft make an uncontrolled landing, but citizens may also be able to assist with the incident.
8. Where there are specific and articulable grounds to believe that the UA will collect evidence of criminal wrongdoing and if the UA will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight.

IMAGE RETENTION:

1. Unless required as evidence of a crime, as part of an on-going investigation, for training, or required by law, images captured by a UA should not be retained by the agency.
2. Unless exempt by law, retained images should be open for public inspection.

ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

Proposal for American Legislative Exchange Council (ALEC)
Unmanned Aerial Vehicle Proposal

Program Objective

The objective of ALEC's Unmanned Aerial Vehicle (UAV) program is to educate our policy makers about the issues surrounding the use of UAVs for domestic purposes. We will inform our state legislator members about considered uses for UAVs in law enforcement, border control, firefighting, search and rescue operations and myriad other uses. We will explore the privacy issues involved and would like to present our members a balanced overview of the topic that addresses some of the misconceptions about UAV capabilities and the benefits of UAV use in the domestic sphere.

Situational Overview

State legislatures are rapidly enacting legislation on domestic UAV use without a complete understanding of the issues involved. As of this writing, 35 states had considered or were considering legislation, including Virginia which passed legislation restricting the use of UAVs, including a two-year moratorium on using UAVs except in university research and search and rescue missions.

State legislators are concerned that UAV surveillance could threaten the civil liberties, especially the privacy of their constituents, so the trend in the legislatures is to err on the side of highly restrictive regulations. Unfortunately, these restrictions might ultimately prevent civilian institutions from taking advantage of UAVs as a cost-effective tool to perform their duties more efficiently during a time of shrinking state budgets. In many cases, ALEC legislators are spearheading these restrictive policies, often due to an incomplete understanding of the issues involved and UAV capabilities.

If misconceptions are not corrected in the immediate future, misguided policy will continue to proliferate throughout state legislatures, and this policy is likely to inform future *national* policy on the domestic use of UAVs. As appropriate UAV implementation could help states meet their public safety objectives in a fiscally responsible way, we would like to see the issues surrounding their use explored in a complete and objective manner.

Program Description

A two-pronged approach would be the most effective way to deal with the issue.

ALEC International Relations Task Force (IRTF) Membership

Model policy on the domestic use of UAVs falls under the jurisdiction of ALEC's International Relations Task Force/National Security Subcommittee, and we anticipate that the task force will consider such policy in the very near future. Issues that capture our members' attention the way this one has are generally brought to ALEC. ALEC task force membership would afford the member

the opportunity to participate in the discussions on the model policy and to inform and enrich the debate. The IRTF is relatively small (well over 100 legislators and 6 private sector members) and has the flexibility to consider and vote on model policy for domestic UAV use rapidly. If this policy is passed within the task force and approved by ALEC's Legislative Board of Directors, it becomes official ALEC model policy and can be accessed by all of our state legislators. Other issues that the task force has explored and continues to discuss include Sequestration, Civilian/Commercial Applications for NASA Research, Sustainable Energy Best Practices in the Military and Overseas, H1B visa expansion, Earth Observation, Expanding the Commercial Marketplace for Space Launches, etc.

The issue of our bimonthly magazine *Inside ALEC* that will be distributed at our Annual Meeting in August 2013 in Chicago will focus on International and Energy issues. An article on domestic uses for UAVs would be a welcome addition to the magazine and would automatically be distributed to those in attendance at the meeting – roughly 1,000 state legislators as well as 1,000 policy and business leaders from across the country. Such distribution would give the issue a deserved spotlight. An article in ALEC's blog, *The American Legislator*, could appear before the Annual Meeting.

UAV Educational Sponsorship Opportunity at ALEC Spring Task Force Summit
ALEC's Communications and Technology Task Force will host a panel discussion/lunch to explore the domestic uses of UAVs at ALEC's Spring Task Force Summit on May 3 in Oklahoma City, OK. We expect 30-40 state legislators to attend. Two speakers who favor more restrictions on the use of UAVs have already been confirmed – Jim Harper a noted privacy expert from the Cato Institute and Ryan Kiesel a noted privacy advocate from the American Civil Liberties Union (ACLU). Both will thoroughly cover the privacy challenges UAV technology poses. This will be our members' first exposure to this issue at an ALEC event, and ALEC wants to ensure that we approach the issue in a balanced fashion. We will have presenters who will emphasize some of the benefits of the domestic uses of UAVs, and the sponsor would be able to select two presenters that would offer this point of view. We would also ask the additional panelists to address the general aviation challenges facing domestic UAVs. We would provide travel expenses for four additional ALEC public sector members from the International Relations Task Force to attend and/or moderate the panel from select states currently considering UAV policy.

Annual Meeting Workshop Sponsorship
This year's Annual Meeting will take place in Chicago, IL August 7-10, 2013 where we expect roughly 2,000 state legislators, policy experts and business leaders to be in attendance. Workshops are panel discussions open to all attendees at our Annual Meeting, and we are confident that a panel discussion on the domestic uses of UAVs would be exceedingly popular. We also have workshop sponsorships at our States and Nation Policy Summit in early December 2013 which generally has attendance of 700-800 state legislators, policy experts and business leaders.

<u>Additional Thoughts</u>
This is a timely issue where our members need a better understanding to make informed decisions. However, this topic is also an excellent opportunity to introduce the concept of civilian applications for products that were originally intended for military and/or space applications and to highlight the critical role that public private partnerships in research play in innovation and economic growth.

AUVSI
ASSOCIATION FOR UNMANNED EHICLE SYSTEMS INTERNATIONAL

2700 South Quincy Street, Suite 400 • Arlington, VA 22206 • 703.845.9671 • 703.845.9679 fax

1 June 2013

COMMENTS OF THE ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL ON THE AEROSPACE STATES ASSOCIATION SUGGESTED PRIVACY LEGISLATION PLAN 2013

I. Executive Summary

The Association for Unmanned Vehicle Systems International (AUVSI)[1] supports the expanded use of unmanned aircraft systems (UAS) and encourages open discussion of privacy concerns and proposed changes to existing rules, regulations, and laws. These discussions should occur concurrently with the integration of UAS into the National Airspace System (NAS)[2] in order to fully realize the benefits of rapidly advancing UAS technology and so that a greater understanding of UAS technology's potential can be achieved. Enactment of legislation now – before sufficient experience with integration of UAS into the NAS exists – is premature, and will hinder the creation and development of this new industry. Barring unnecessary delays, AUVSI estimates that this new industry is poised to create over 70,000 new jobs and $13.6 billion in economic impact within the first three years of integration alone.[3]

New legislation at the federal or state level that is not technology neutral or that is inconsistent with existing privacy rules, regulations, and laws would stifle innovation and cause delay, and may prevent or discourage the use of UAS by public safety agencies and other potential users. Fourth Amendment jurisprudence, existing federal and state privacy laws, and comprehensive Federal Aviation Administration (FAA) regulations already provide extensive guidance that would allow for initial integration of UAS operations. The FAA, for example, has taken steps to address privacy concerns relating to the use of UAS at test sites, which will help gather knowledge and best practices about UAS operations. If the FAA completes its required and pending rulemaking activities for UAS integration, there will be ample opportunities for multi-stakeholder input.

II. Existing Fourth Amendment Protections

The Fourth Amendment and related case law already governs UAS operations by government users, ensures accountability, and guides the use of aircraft in which the cockpit and pilot are on the ground. Federal, state, and local government agents must obtain search warrants when their use of any technology, including UAS, may violate an individual's reasonable expectation of privacy protected by the Fourth Amendment.[4] These protections are well-established and address many different privacy concerns relating to government adoption and use of advancing technologies, such as UAS. For more than 220 years, the Fourth Amendment has been applied to new technologies used in warrantless

[1] AUVSI – the world's largest non-profit organization dedicated to the advancement of unmanned systems – represents more than 7,000 members from 55 allied countries and 2,500 organizations involved in fields of government, industry and academia.

[2] The FAA Modernization and Reform Act of 2012 requires FAA to safely integrate UAS into the NAS by September 2015, and mandates, among other things, the creation of UAS test sites and rulemaking proceedings addressing the integration of civil UAS operations. P.L. 112-95, §§ 331-334, 126 Stat. 11, 72-77 (2012).

[3] AUVSI, *The Economic Impact of Unmanned Aircraft Systems Integration in the United States* (Mar. 2013), at 2, http://www.auvsi.org/econreport.

[4] *See Katz v. United States*, 389 U.S. 347 (1967).

observations – including several Supreme Court decisions on aerial observations[5] and, more recently, thermal imaging[6] and GPS technologies[7] – and it will continue to be applied to UAS and other future technologies that have not yet been invented. The Court, in a 2013 decision, held that law enforcement use of a highly-trained drug sniffing dog, roaming outside a home, was "an unlicensed physical intrusion" distinguishable from "Girl Scouts and trick-or-treaters," and was thus an unreasonable search.[8] UAS technology is not so distinct from other advanced technologies as to require supplemental legislation.[9] On the contrary, UAS-specific legislation and laws may have unintended effects, including confusing and complicating the application of existing search warrant requirements[10] that have been carefully developed over two centuries.

AUVSI strongly supports the International Association of Chiefs of Police (IACP) recommended guidelines for UAS operations and associated data collection,[11] which the Airborne Law Enforcement Association (ALEA)[12] and others have adopted and even the American Civil Liberties Union (ACLU) has praised.[13] Like IACP, AUVSI recognizes the "proven effectiveness" of UAS and that the "potential benefits [to public safety] are irrefutable."[14] AUVSI opposes any legislation that hamstrings first-responders.

III. FAA's Approach to Privacy and Rulemaking

The Congressionally-mandated FAA rulemaking processes for the integration of small UAS (sUAS) will provide ample opportunities for the public to comment on privacy issues relating to UAS operations.[15] Unlike government operators, who are permitted to operate UAS, albeit through a cumbersome process,[16] civilian operators have no practical, legal means of doing so until the FAA

---

[5] *See Florida v. Riley*, 488 U.S. 445 (1989) (naked-eye observations through greenhouse roof from helicopter at 400 feet not an unreasonable search); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (precision aerial photographs of industrial complex from 1,200-12,000 feet not a prohibited search); *California v. Ciraolo*, 476 U.S. 207 (1986) (no reasonable expectation of privacy from naked-eye observations of yard from fixed-wing aircraft flying at 1,000 feet).

[6] *See Kyllo v. United States*, 533 U.S. 27 (2001) (warrantless use of thermal imaging device to see heat emanating from inside home deemed an unreasonable search).

[7] *See United States v. Jones*, 132 S. Ct. 945 (2012) (month-long tracking with GPS required a warrant).

[8] *Florida v. Jardines*, 133 S.Ct. 1409, 1415 (2013).

[9] "In combination, however, [the *Ciraolo, Riley, Dow Chemical, Kyllo and Jones*] rulings indicate that the Fourth Amendment is likely to provide significantly more protection from government UAS observations than is commonly assumed." John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL'Y 457, 516 (2013).

[10] *See* Richard M. Thompson II, CONG. RESEARCH SERV., R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Apr. 3, 2013), at 18-21 (reviewing several bills that "establish arguably greater constraints on [UAS] usage than the Fourth Amendment requires." *Id.* at 18).

[11] IACP, *Recommended Guidelines for the Use of Unmanned Aircraft* (Aug. 2012) ("IACP Guidelines").

[12] ALEA, *Resolution in Support of the International Association of Chiefs of Police Aviation Committee's Recommended Guidelines for the Use of Unmanned Aircraft* (Aug. 29, 2012), http://www.alea.org/assets/cms/files/Resolutions/In%20Support%20of%20UAS%20Guidelines.pdf.

[13] *See* Jay Stanley, *Police Chiefs Issue Recommendations on Drones: A Look at How they Measure Up*, ACLU (Aug. 17, 2012, 9:39 AM), http://www.aclu.org/blog/technology-and-liberty/police-chiefs-issue-recommendations-drones-look-how-they-measure.

[14] IACP Guidelines, at 1. What appears to be the first documented instance of a human life being saved with a UAS occurred in Canada earlier this year. *See Single Vehicle Rollover - Saskatoon RCMP Search for Injured Driver with Unmanned Aerial Vehicle,* ROYAL CANADIAN MOUNTED POLICE (May 9, 2013), http://www.rcmp-grc.gc.ca/sk/news-nouvelle/video-gallery/video-pages/search-rescue-eng.htm. It will certainly not be the last.

[15] P.L. 112-95, § 332 (requiring the sUAS and integration final rules by August 14, 2014 and December 14, 2015, respectively).

[16] FAA, *Unmanned Aircraft Systems (UAS): Certifications and Authorizations*, http://www.faa.gov/about/initiatives/uas/cert/; *see also* Felicity Barringer, *F.A.A.'s Concerns Hold Up Use of Wildfire Drones*, N.Y. TIMES (May 21, 2013), http://www.nytimes.com/2013/05/22/us/faas-concerns-hold-up-use-of-wildfire-

completes its legally required, and long-delayed, rulemakings.[17] Recognizing the importance of addressing privacy concerns, the FAA has taken extraordinary measures to permit public participation in determining the privacy policies that will govern UAS test sites – the agency's first major step toward integration.[18] Indeed, FAA "aim[ed] 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 operators should respond to those issues in the long run."[19] Rather than passing uninformed[20] and potentially unenforceable[21] legislation now, Congress and state lawmakers should wait for the FAA to complete its rulemaking processes.

The FAA's primary mission is, and must remain, aviation safety. Still, insofar as privacy issues are inextricably linked to the agency's creation of a regulatory framework for the integration and operation of UAS, the FAA rulemaking process is the appropriate forum to address privacy concerns. The FAA has properly recognized the role that federal and state law enforcement agencies play in enforcing laws regarding the protection of an individual's right to privacy, as well as its complementary authority to revoke or suspend a UAS operator's license. Like the Fourth Amendment jurisprudence applicable to public UAS operators, analogous state laws relevant to civil operators that "address trespass, invasion of privacy, harassment, and stalking [are] well established."[22] AUVSI supports the FAA's position that Fair Information Practice Principles (FIPPs) should inform UAS privacy policies on the collection, storage, and use of data.[23] Clearly, the registration of certain UAS and pilots with the FAA, the equipage of UAS with identification/position broadcast capability, and the guidelines set forth in AUVSI's UAS Operations Code of Conduct[24] could all contribute to the creation of an overall approach to managing privacy concerns. FAA rulemaking proceedings are the proper forum to address all of these important considerations.

IV. Conclusion

AUVSI supports the integration of UAS into the NAS in a safe and responsible manner, while safeguarding the existing right to privacy and ensuring transparency and accountability. Existing federal and state privacy protections should extend to the operations of UAS, just as they do to the operations of any other advanced technology. But before consideration of any supplemental technology neutral privacy legislation, the FAA should be allowed to gain experience through the UAS test site program and to then complete the well-established regulatory processes for UAS integration that Congress has already mandated. Fourth Amendment jurisprudence, federal and state privacy protections, and other existing laws and regulations are sufficiently robust to guide this effort.

---

drones.html?_r=0.

[17] *See* Alissa M. Dolan and Richard M. Thompson II, CONG. RESEARCH SERV., R42940, *Integration of Drones into Domestic Airspace: Selected Legal Issues* (Apr. 4, 2013), at 4 (internal citations omitted). Indeed, the FAA's sUAS notice of proposed rulemaking has already been delayed more than two years beyond the agency's initially projected publication date of March 10, 2011. DEPT. TRANSP., *Report on DOT Significant Rulemakings* (May 10, 2013), at 13.

[18] *See* Unmanned Aircraft Test Site Program, 78 Fed. Reg. 12,259 (Feb. 22, 2013); *see also* FAA, *Transcript of Online Session on UAS Test Site Privacy Policy* (Apr. 3, 2013), http://www.faa.gov/about/initiatives/uas/media/UAStranscription.pdf.

[19] 78 Fed. Reg. at 12,260.

[20] *See supra* note 9, at 517 (contrasting UAS with other emerging technologies in that the focus on privacy concerns has come before the benefits are widely recognized).

[21] *See supra* note 17, at 27-29 (noting that state and local regulation of UAS may be subject to challenge on federal preemption grounds).

[22] *See supra* note 9, at 514.

[23] 78 Fed. Reg. at 12,260.

[24] http://www.auvsi.org/conduct.

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Unmanned Aircraft System Operations

Industry "Code of Conduct"

The emergence of unmanned aircraft systems (UAS) as a resource for a wide variety of public and private applications quite possibly represents one of the most significant advancements to aviation, the scientific community, and public service since the beginning of flight. Rapid advancements in the technology have presented unique challenges and opportunities to the growing UAS industry and to those who support it. The nature of UAS and the environments which they operate, when not managed properly, can and will create issues that need to be addressed. The future of UAS will be linked to the responsible and safe use of these systems. Our industry has an obligation to conduct our operations in a safe manner that minimizes risk and instills confidence in our systems.

For this reason, the Association for Unmanned Vehicle Systems International (AUVSI), offers this Code of Conduct on behalf of the UAS industry for UAS operation. This code is intended to provide our members, and those who design, test, and operate UAS for public and civil use, a set of guidelines and recommendations for safe, non-intrusive operations. Acceptance and adherence to this code will contribute to safety and professionalism and will accelerate public confidence in these systems.

The code is built on three specific themes: Safety, Professionalism, and Respect. Each theme and its associated recommendations represent a "common sense" approach to UAS operations and address many of the concerns expressed by the public and regulators. This code is meant to provide UAS industry manufacturers and users a convenient checklist for operations and a means to demonstrate their obligation to supporting the growth of our industry in a safe and responsible manner. By adopting this Code, UAS industry manufacturers and users commit to the following:

Safety

- We will not operate UAS in a manner that presents undue risk to persons or property on the surface or in the air.
- We will ensure UAS will be piloted by individuals who are properly trained and competent to operate the vehicle or its systems.
- We will ensure UAS flights will be conducted only after a thorough assessment of risks associated with the activity. This risks assessment will include, but is not limited to:
    - Weather conditions relative to the performance capability of the system

- Identification of normally anticipated failure modes (lost link, power plant failures, loss of control, etc) and consequences of the failures
- Crew fitness for flight operations
- Overlying airspace, compliance with aviation regulations as appropriate to the operation, and off-nominal procedures
- Communication, command, control, and payload frequency spectrum requirements
- Reliability, performance, and airworthiness to established standards

Professionalism

- We will comply with all federal, state, and local laws, ordinances, covenants, and restrictions as they relate to UAS operations.
- We will operate our systems as responsible members of the aviation community.
- We will be responsive to the needs of the public.
- We will cooperate fully with federal, state, and local authorities in response to emergency deployments, mishap investigations, and media relations.
- We will establish contingency plans for all anticipated off-nominal events and share them openly with all appropriate authorities.

Respect

- We will respect the rights of other users of the airspace.
- We will respect the privacy of individuals.
- We will respect the concerns of the public as they relate to unmanned aircraft operations.
- We will support improving public awareness and education on the operation of UAS.

As an industry, it is incumbent upon us to hold ourselves and each other to a high professional and ethical standard. As with any revolutionary technology, there will be mishaps and abuses; however, in order to operate safely and gain public acceptance and trust, we should all act in accordance with these guiding themes and do so in an open and transparent manner. We hope the entire UAS industry will join AUVSI in adopting this industry Code of Conduct.

ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

May 31, 2013

Mr. Robert Davis
Cadwalader, Wickersham & Taft LLP
700 6th Street, NW, Suite 300,
Washington, DC 20001

Lt. Gov. Mead Treadwell
The Aerospace States Association
107 S. West Street, Suite 510
Alexandria, VA 22314

Dear Mr. Davis and Lieutenant Governor Treadwell,

Thank you for the invitation to participate in the Aerospace States Association's efforts to draft model privacy legislation to regulate unmanned aerial systems (UAS).

EFF is a non-profit organization that has worked for more than 20 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. Our organization has, for the last few years, been extensively involved in privacy and civil liberties issues raised by unmanned aircraft (UA),[1] commonly referred to as drones. This work has included consulting with state and federal legislators on legislation that would place appropriate limits on law enforcement's abilities to use drones for surveillance; commenting on government and private use of drones on EFF's website, in the press, and in other public fora; and obtaining, reporting on and making accessible to the public drone authorization records received from the FAA pursuant to the Freedom of Information Act.[2]

Legislation regulating drone use to protect privacy must, at a minimum, address three main points:

1. Law enforcement use of drones requires a warrant;
2. Commercial drone use must be subject to privacy protections and reporting requirements;
3. Regulations on private and media use of drones must strike an appropriate balance between the First Amendment and privacy.

Law Enforcement Drone Use Requires a Warrant
UAS have the potential to fundamentally change the nature of policing in the United States. The technological advances in surveillance provided by drones may provide important benefits to law enforcement. For example, drones could be employed in dangerous situations to avoid risk of harm to an officer or to search in areas challenging to traverse. Drones will also make aerial surveillance much less costly for cash-strapped law enforcement agencies.

---

[1] For links to EFF's drone-related work, s*ee generally Drone Flights in the U.S.,* EFF.org, https://www.eff.org/foia/faa-drone-authorizations.

[2] *See* Jennifer Lynch, *Are Drones Watching You?*, EFF.org (Jan. 10, 2012) https://www.eff.org/deeplinks/2012/01/drones-are-watching-you.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 *fax* +1 415 436 9993 *web* www.eff.org *email* information@eff.org

However, these same advances will also present significant privacy and civil liberties risks. UAS are capable of highly advanced and near-constant surveillance through live-feed video cameras, thermal imaging, communications intercept capabilities, and backend software tools such as license plate recognition, GPS tracking, and facial recognition. They can amass large amounts of data on private citizens, which can then be linked to data collected by the government and private companies in other contexts. Without strong limitations on how this sophisticated technology can be used, we risk a society where we may all be subject to government surveillance at any time.

For this reason, any legislation regulating law enforcement UAS use must require that officers obtain a warrant based on probable cause before using the UAS for criminal investigations. Such a warrant must have limitations on duration and content recorded, much like a wiretap order does today,[3] and must apply whether the drone flies over private or public space.[4] The warrant requirement must also apply when law enforcement seeks access to data gathered by a drone that is owned or flown by a separate entity, whether that entity is a private party, commercial entity or another public agency.[5]

The warrant requirement can only be subject to limited exceptions for emergency situations such as imminent threats to life or of great bodily harm and only where a warrant could have been obtained but for the time constraints of the situation. And legislation establishing a warrant requirement must have a meaningful enforcement mechanism that allows persons subject to drone surveillance to move to suppress the evidence in any case brought against them.

Commercial Drone Use Must Be Subject to Privacy Protections and Reporting Requirements

Congress has mandated that by 2015, the skies will be open to commercial drone flights.[6] In fact, the FAA has predicted that, in addition to the hundreds of drones currently used domestically by the military and law enforcement, there will be roughly 10,000 commercial drones flying in the US skies in just five years.[7] In reality, many small drone operators are already flying UAVs for

---

[3] *See, e.g., Berger v. New York*, 388 U.S. 41 (1967) (describing particularity requirements for wiretap warrants). In *Berger*, the Supreme Court indicated that the Fourth Amendment triggers heightened scrutiny when surveillance is undertaken as "a series or a continuous surveillance" rather than as "one limited intrusion." *See id.* at 57. Therefore, a statute that regulates "a series or a continuous surveillance" must include special privacy protections or risk invalidity under the Fourth Amendment. *See id.* at 56.

[4] *See, e.g., U.S. v. Jones*, 132 S.Ct. 945 (2012) (Alito, J., concurring; Sotomayor, J. concurring) In *Jones*, which held law enforcement must get a warrant before affixing a GPS tracking device to a car, five justices took issue with the pervasive nature of surveillance possible with the device, even though the device tracked travel that occurred in public.

[5] Legislatures must also establish laws limiting the use of drones by non-law enforcement public agencies such as departments of forestry or agriculture. These should include requirements that images, footage or data pertaining to humans obtained by a public agency should not be disseminated outside the collecting agency and should not be used for purposes other than that for which it was collected. And all public agencies, including law enforcement, should be subject to annual reporting requirements to the public on any UAV purchases and how UAVs have been used.

[6] *See* FAA Modernization and Reform Act of 2012, Pub. L. 112–95.

[7] *FAA Aerospace Forecast Fiscal Years 2012-2032: Unmanned Aircraft Systems, available at* http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/media/Unmanned%20Aircraft%20Systems.pdf.

commercial purposes.[8]

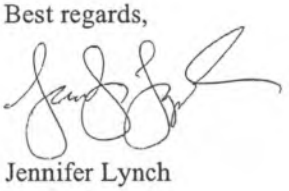
For these reasons, it is critical that legislatures enact laws establishing privacy protections for commercial drone flights. These laws should set out standards that limit the collection, use, sharing, retention and disclosure of data gathered by UAVs. They should also include requirements that the commercial entity establish notice procedures on the type of data gathered by a UAV, how it's gathered and for what purpose, as well as the location the UAV is flown, how long data is retained, with whom it's shared, and how it's disclosed.[9]

Balancing the First Amendment and Privacy in Private and Media Use of Drones
Regulations on private and media use of drones need to strike a balance between protecting privacy and not hampering First Amendment protected speech and associated activities.

As UAV use becomes more prevalent throughout society, private parties and the media will likely also want to fly UAVs for their own and for newsgathering purposes. Some of these activities might include using a UAV to report on a public figure, to monitor law enforcement activities at a political rally, or to record the aftermath of a natural disaster in an urban area. Each of these may impact privacy interests—of the public figure, of the police officer, or of the victims of the natural disaster—but also involve First Amendment-protected activities.[10] For this reason, any law designed to protect privacy must be sufficiently cabined to provide room for these activities. Acceptable limitations could include, for example, duration limits (such as limitations on how long a drone may be used to monitor a specific person), location limits (such as restrictions on monitoring of private spaces like a home or backyard) or could require a finding that the monitoring impinges on an objectively reasonable privacy interest, is highly offensive to a reasonable person, and causes emotional distress.

Conclusion
EFF welcomes the ASA's efforts to craft model legislation to regulate public and private drone use. Please let me know if I can answer any questions or provide further information.

Best regards,



Jennifer Lynch
Staff Attorney
Electronic Frontier Foundation

---

[8] *See, e.g.,* Chris Francescani, *From Hollywood to Kansas, Drones are Flying Under the Radar*, Reuters (Mar 3, 2013) http://www.reuters.com/article/2013/03/03/us-usa-drones-domestic-idUSBRE92206M20130303.

[9] *See, e.g.,* Drone Aircraft Privacy and Transparency Act of 2013, H.R. 1262, 113th Cong. 1st Sess. (1st Sess. 2013) § 339 (b).

[10] For more information, *see, e.g.,* Bill Kenworthy, *Photography & the First Amendment*, First Amendment Center (Jan. 1, 2012), http://www.firstamendmentcenter.org/photography-the-first-amendment; Alissa Dolan & Richard Thompson, *Integration of Drones into Domestic Airspace: Selected Legal Issues*, 17-19, Congressional Research Service (Apr. 4, 2013) *available at* http://www.fas.org/sgp/crs/natsec/R42940.pdf.

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Statement of

Amie Stepanovich, Director
EPIC Domestic Surveillance Project[1]

for the

Aerospace States Association

regarding

Privacy Legislation Plan 2013

May 31, 2013

On February 14, 2012, President Barack Obama signed the Federal Aviation Administration Reauthorization Act of 2012 ("FAA Act"). The Act provided for funding for the Federal Aviation Administration ("FAA"), advanced the Next Generation Air Transportation System ("NextGen"), and implemented several other aviation-related provisions to increase air traffic safety and reduce accidents.

The FAA Act also provided for the increased and expedited licensing of drones within the United States National Airspace System ("NAS"). Prior to the FAA Act, drones licenses were uncommon, and could only be obtained by a government entity, or, even more rare, by a private entity with an "experimental" limitation. Less than seven formatted pages in length, the relevant sections of the FAA Act fail to address many of the problems inherent in increased domestic drone use. The most significant of these issues is that of privacy.

There are significant privacy concerns involved in the use of drones over domestic soil. Drones are uniquely designed to carry invasive technology that may potentially erode the rights of individuals in the United States to be free of government surveillance under the Fourth Amendment of the Constitution. In addition, drones operated by private entities open new doors to spying, harassment,

[1] EPIC law clerks Adam Marshall and Heather Nodler helped with the drafting of this statement.

and stalking that are not addressed under current law. Finally, the failure of the FAA to implement a drone licensing system that implements the principles of transparency and public access means that many of these intrusions into our private lives will go unnoticed and undocumented.

EPIC'S PETITION TO THE FEDERAL AVIATION ADMINISTRATION

In February 2012, EPIC, joined by over 100 organizations, experts, and members of the public, petitioned the FAA to consider privacy as a key factor in its efforts to streamline and increase drone licensing in the United States. The FAA responded to EPIC's petition in February 2013 and agreed to make privacy a primary factor in its selection of six nationwide test sites for drones in the United States. The FAA requested public comment on its proposed privacy policy and guidelines for these test sites. In response, EPIC asked the FAA to maintain a public database for drone operators, including their geographic area of operation and the surveillance equipment that the drone will carry. EPIC also asked that the FAA implement data collection and retention policies to ensure public notice of domestic drone surveillance operations.

The FAA's actions indicate that the Agency has recognized that new protections are necessary to remedy the privacy threats proposed by drone surveillance. Effective solutions require affirmative action not only from the FAA, but also from other federal agencies and law enforcement bureaus seeking to operate drones domestically, state and local governments, and Congress.

DEVELOPMENTS IN THE STATES

There has been a recent surge in state drone legislation. In total, 43 states have introduced laws that relate to drone surveillance and privacy. Governors of six of these states have now signed measures into law, including Florida, Idaho, Montana, North Dakota, Tennessee, and Virginia. Moreover, six additional states have adopted resolutions on drones: Alabama, Alaska, Idaho, Indiana, Nevada, and Pennsylvania. A drone law in Texas has passed both chambers and awaits the Governor's signature.

The laws in Florida, Tennessee, and Idaho define what drones are and restrict drone use by law enforcement. They require either a warrant or an emergency situation. In Idaho, the law also allows drone use with reasonable suspicion of criminal conduct. The proposed Texas law details numerous situations in which law enforcement may use drones, with and without a warrant. The laws in Florida, Tennessee, and Montana limit the admissibility of evidence obtained by drones, with the standard varying from requiring a warrant to reasonable suspicion.

The law passed in Idaho and the proposed Texas laws restrict private drone use. The Texas draft law carves out numerous exceptions for both public and private use, including border security, mapping, scholarly research, real estate brokerage,

and maintenance of utilities. The laws in Florida, Tennessee, Montana, Virginia, and North Dakota place no restrictions on private use.

The laws in Florida, Idaho, Tennessee, and Texas are written to provide remedies for parties harmed by improper drone use.

In April 2013, Virginia passed legislation prohibiting the use of drones by state agencies dealing with law enforcement or regulatory violations. There are exceptions for Amber and Blue Alerts, search and rescue operations, and uses by the National Guard and educational institutions. The ban lasts until July 2015. In the interim, state agencies have been asked to develop model protocols for drone use. The Alaska and Indiana legislatures have also adopted resolutions calling for the creation of drone task forces to study and make recommendations on their use.

A bill in North Dakota was recently sent to the Governor that would apportion one million dollars to pursue having the FAA designation as a drone test site, and an additional four million in operations funds if it is chosen.

EPIC'S RECOMMENDATIONS TO CONGRESS

In testimony before the Senate Judiciary Committee in 2013, EPIC proposed numerous recommendations for protections that Congress could adopt in order to build privacy protections in to U.S. drone operations. These recommendations include:

- A requirement for drone operators to submit detailed public reports on drones' intended use. Issuance of a license should be contingent on the completion of this reporting, and a privacy right of action and other penalties should ensure that the operators' behaviour complies with the representations made in the report;

- Warrant requirements for law enforcement use of drones, with narrow exemptions for exigent circumstances. The use of drones by law enforcement should be subject to mandatory public reporting requirements, such as those found in the Wiretap Act;

- A prohibition on broad and untargeted drone surveillance by law enforcement;

- A federal Peeping Tom statute, recognizing the enhanced capabilities of aerial drones, should be implemented in order to provide baseline privacy protections for individuals in the home;

- Random independent audits and third-party oversight should be mandated for all drone operators within the United States.

As drone surveillance technology continues to leap ahead, the United States needs to be ready with accompanying measures to ensure that individual rights are not eroded. EPIC looks forward to participating in a public conversation about how to best protect privacy and civil liberties in the development and sue of drones throughout the Country.

RESOURCES

- EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, http://epic.org/privacy/drones/.

- EPIC Spotlight on Surveillance, *"Unmanned Planes Offer New Opportunities for Clandestine Government Tracking"* (Aug. 2005), http://epic.org/privacy/surveillance/spotlight/0805/.

- EPIC, *Comments to the Federal Aviation Administration of the Department of Transportation* (April 23, 2013), http://epic.org/privacy/drones/EPIC-Drones-Comments-2013.pdf.

- EPIC, *Comments to the Federal Aviation Administration of the Department of Transportation* (May 8, 2012), http://epic.org/apa/comments/EPIC-FAA-2012-0252.pdf.

- *Hearing on "Using Unmanned Arial Systems Within the Homeland: Security Game Changer?" Before the Subcomm. on Oversight, Investigations, and Management of the H. Comm. on Homeland Security*, 112th Cong. (2012) (statement of Amie Stepanovich, Associate Litigation Counsel, Electronic Privacy Information Center), *available at* http://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf.

- *Field Forum on the Impact of Domestic Use of Drone Technology on Privacy and Constitutional Rights of All Americans, Sanctioned by the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. (2012) (statement of Amie Stepanovich, Associate Litigation Counsel, Electronic Privacy Information Center), *available at* http://epic.org/privacy/drones/EPIC-Drones-Testimony-102512.pdf.

- EPIC, *Domestic Drones Petition* (March 2013), http://epic.org/drones_petition/.

- EPIC *Petition to the Federal Aviation Administration* (Feb 24, 2012), http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.

Douglas Marshall ASA Privacy

Two major issues have captured the public's attention over the last two years regarding unmanned aerial vehicles (UAVs), (also known as UAS, or unmanned aircraft systems, RPAs, or remotely piloted aircraft, or "drones," as they are often misleadingly referred in the mass media). The first is the controversial use of UAV-launched missiles and bombs to neutralize threats to U.S. security from terrorists or others hostile to the United States, which have included U.S. citizens. The second arises from concerns over potential violations of privacy or indiscriminate, warrantless surveillance by law enforcement agencies using small, non-tactical fixed-wing or rotorcraft UAVs. A related concern is the perceived threat that U.S. intelligence agencies and military units will "bring home" the sophisticated ISR (Intelligence, Surveillance, Reconnaissance) UAVs that are currently used for counterterrorism and military operations in theater and deploy them to spy on U.S. citizens (although such activity is clearly prohibited by federal law).

Caught up in the whirlwind of popular culture, media hysteria, and political forces is a large international community of scientists, researchers, government agencies and civilian or private operators of UAS who promote and support the peaceful use of the technology for a wide variety of humanitarian and potential commercial applications that have nothing to do with law enforcement or national defense and security.

By way of example, the Arctic is a critically important environment, exerting strong influence on the global climate. The effect of climate change is exaggerated in the Arctic, and, as a result, the Arctic region (north of the Arctic Circle, $66^0\,33'$N latitude) is undergoing very rapid change. Because of these rapid changes, scientists are urgently trying to understand the many climate processes and mechanisms of the Arctic. Use of UAS for environmental research in the Arctic has been ongoing since 1999, and continues to this day. More examples of scientific applications of UAS abound, and a comprehensive list would fill a multi-page appendix.

As a result of similar activities around the globe, the UAS sector has been a growth industry for over a decade, fueled primarily by the Department of Defense and the U.S. intelligence services, but supplemented by a rapidly growing civilian sector devoted to non-military applications such as law enforcement, agricultural remote sensing, atmospheric science, wildlife management, power line and pipe line inspection, fisheries observation and enforcement, border protection, firefighting, flood protection, disaster response, and the like.

A major challenge for the UAS community is identifying the public policies that should drive the next phase of technical development, and, more recently, the influence that the question of personal privacy should have, if any, in the evolution of those policies. State and local governments are grappling with the role that government should or will play in this public debate. The choices for local and state government are: To be active advocates for UAS technology, thereby supporting the anticipated economic impacts from the creation of highly skilled, high paying jobs, but taking no position on the legal and privacy issues; to devote the necessary time

and resources to develop a model privacy policy that could be adopted by other governmental entities; or to do nothing and take no position on privacy, thereby conceding the policy question to the federal government or the private sector.

The issue of privacy and the potential for invasions of personal privacy by individuals and/or government by the use or misuse of remotely piloted aircraft equipped with cameras and other surveillance devices has generated proposed legislation, both state and federal, and aggressive publicity campaigns intended to drastically limit or even outlaw RPAs for any purpose whatsoever. Indeed, the "right to privacy," or the "right to be let alone," has been recognized by the U.S. Supreme Court in a number of cases as being among the fundamental rights guaranteed American citizens by the U.S. Constitution. The seminal treatment of the subject was an article published in the Harvard Law Review, authored by Louis Brandeis and Samuel Warren ("The Right to Privacy" HLR 4, no. 5 (1890): 193-220), in which the authors argued that the time had come for the courts to recognize a common law right to privacy. The article can be read today with virtually no changes and still be as relevant and prescient as it was in 1890.

In our age of electronic exhibitionism and voyeurism, it can be argued that privacy no longer has the meaning that it did over 75 years ago when laws were passed to prohibit the government from wiretapping telephones without a search warrant (although illegal wiretapping in violation of the requirements of the Fourth Amendment apparently still occurs). Dean Prosser's four invasion of privacy torts (intrusion upon a person's seclusion or solitude, or into his private affairs; public disclosure of embarrassing private facts about a person; publicity that places the person in a false light in the public eye; and appropriation, for the someone's advantage, of another person's name or likeness), are no less important concepts now than they were when he described them in his landmark article in the California Law Review over 50 years ago (*Privacy,* 48 Calif. L. Rev. 383 (1960)). But these four categories of invasions of privacy are civil wrongs that provide the basis for an award of monetary damages against the violator. The current media-driven angst over the potential for privacy intrusions from the utilization of unmanned aircraft by law enforcement agencies at all levels (federal, state and local) seems to derive from fear of "Big Brother" (apologies to Orwell) type of broad area, warrantless surveillance of the general population, although no law enforcement agency has publicly stated that it has any intention of ever using UAS for that purpose. Yet, manned aircraft (primarily helicopters), have been used for decades for that precise purpose, with little objection from the public. News helicopters hover over every event from a traffic jam in Los Angeles to a natural disaster in Oklahoma, state highway patrols enforce speed limits with aviation assets, and police departments and first responders routinely use aircraft (often equipped with cameras) to support their law enforcement and firefighting activities.

Some also argue that there is no fundamental difference between carrying a high resolution or infrared camera or some other sensing device on a UAS and deploying the same payload on a manned aircraft, and the Supreme Court has repeatedly held

that observations of law violations from a manned aircraft in the navigable airspace do not violate the Fourth Amendment, even when a warrant is not first obtained.

As a result of pressures applied to legislators, local governments and policy makers by these diverse interests, laws have been proposed in a number of states that are intended to either restrict the use of UAS in many applications or ban them outright, whether the intended use is by law enforcement agencies, or civilians. The FAA has been compelled to conduct public forums on the privacy issue as a result of language in the FAA Modernization and Reform Act of 2012, and is being pressured to propose rules or publish guidelines dealing with the privacy issue.

Thus, the evolving legal issue is whether any local legislation can legitimately regulate an activity that heretofore has fallen under the exclusive jurisdiction of the Federal Aviation Administration. A related policy issue is whether the FAA's statutory mandate dictates that it should have any interest in privacy, or whether it should limit its oversight to traditional aviation concerns such as safety, airworthiness, certification, production standards and airspace rules. The overarching issue is whether there should be any legal restrictions beyond the Fourth and Fifth Amendments on the use of unmanned aircraft by law enforcement agencies or private individuals or entities.

The principle stakeholders in the ongoing privacy debate are a diverse and sometimes unlikely assortment of advocacy partners, often entities or organizations that might ordinarily occupy opposite extremes in philosophy, joining forces to oppose something that they both find threatening or unacceptable. At one extreme lies the UAS industry, represented by many small entrepreneurs, as well as the large defense and aerospace concerns that largely serve the needs of the U.S. military and intelligence services. At the other extreme are civil liberties advocates such as the ACLU, EPIC (Electronic Privacy Information Center), EFF (Electronic Frontier Foundation) and others, who represent the concerns for potential intrusions into personal privacy by government, as well as private citizen exploitation of technology to engage in spying, eavesdropping, data mining, and identity and financial data theft, among others. In the middle of the debate resides the FAA, which has jurisdiction over all activities in the navigable airspace of the U.S.

Potential customers of the industry consist of public safety agencies desiring to acquire small UAS as affordable supplements to existing law enforcement and first responder technology; state and federal science and technology agencies that view UAS as an additional tool to carry out their missions; public and private research universities that similarly seek the use of the technology for a wide variety of research purposes; and, advocacy organizations like AUVSI whose members are engaged in the research and development of this rapidly evolving technology.

The stakeholders are many, the issues are fundamental, and the collective wisdom of all concerned will be needed to solve the problem. ASA is an ideal facilitator to fill that role.

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
COMMENTS ON PROPOSED DRONE LEGISLATION
MAY 31, 2013

Use of Domestic Drones

The increasing number of bills introduced in states across the country addressing the use of unmanned aerial vehicles, also known as drones, signal that not only are states concerned with intrusive government surveillance of their citizens without a warrant, but that domestic drone use is becoming more prevalent as the technology advances, signaling a sudden need for legislation. There are major Fourth Amendment and privacy implications that come with the use of drones in the United States, and the threats to privacy and civil liberties need to be properly addressed in any new drone legislation. Many outdated statutes are applied today in the digital age that undercut Fourth Amendment rights, and new regulations need to address the concerns of these rapidly advancing surveillance tools. That is why the National Association of Criminal Defense Lawyers (NACDL) created its own model legislation, promoting protection of fundamental Fourth Amendment rights. The model legislation is available here.[1]

Prohibited Use Without a Warrant and Suppression of Evidence

If drones are used by a person or entity of the government or funded in any way by the government, a warrant should be required for any surveillance of a person within a state, county, or municipality. A warrant should also be required for the surveillance of personal or business property located within the state to gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation, except in certain special circumstances. This prevents unwanted government intrusion into privacy, and protects Fourth Amendment and state privacy rights. Traditionally, an exception to the warrant requirement exists for evidence that is found in "plain view." The plain view doctrine becomes muddled, however, when drones are used because the drones have high-tech capabilities, that are not in the "general public use,"[2] to conduct surveillance on areas in plain view and not in plain view, such as the inside of a home.[3] The technology is evolving so rapidly that it is currently difficult to discern exactly what kind of private data may be collected by the government and private entities. Unmanned aircrafts may be outfitted with surveillance equipment to include high resolution cameras, thermal heat imaging devices, and geolocation tracking devices.

Additionally, any evidence obtained in violation of the legislation should be inadmissible in a criminal trial. It is important that this suppression remedy be included in state drone legislation, otherwise the only recourse an individual could have is civil, which does not benefit a defendant facing criminal charges. A warrant requirement may be toothless without such a suppression remedy.

Limit Exigent Circumstances

Reasonable exceptions to a warrant requirement for the use of a surveillance drone include exigent circumstances or the assessment of an environmental or weather related catastrophe. Exigent

---

[1] http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=26568&libID=26537.
[2] Kyllo v. United States, 533 U.S. 27, 34 (2001) (reasoning that the police used a device, a thermal heat imaging device, not in the "general public use" to gather information about the inside of a private home.).
[3] *Id.* (holding that using thermal imaging to obtain information from inside a home constituted a search under the Fourth Amendment.).

circumstances exist when law enforcement possesses reasonable suspicion that absent swift preventative action, there is an imminent danger to life or imminent risk of threat or bodily harm. This should further be limited for use only until the danger and risk that prompted the use of the drone are no longer imminent.

Access to Third Party Records

Drone legislation should address the "third party doctrine." Third party records are records created and stored by private companies in their ordinary course of business. Today, these records go beyond bank records or dialed phone numbers, and can include all emails, geo-location information, a record of visited websites, and even internet search terms. The Supreme Court has held that individuals have no reasonable expectation of privacy in records shared or generated by a third party. By giving up information to a third party, a person "assumes the risk" that the company would reveal that information to the government. In other words, law enforcement may be able to access drone surveillance data, without a warrant, obtained by a private company for use as evidence in a criminal trial.

In a recent Supreme Court decision, *United States v. Jones*, which involved the placement of a GPS locator on a suspect's car by police officers without a valid warrant, the Court held that the use of a GPS device constituted a search under the Fourth Amendment.[4] Justice Sotomayor's concurrence in particular questioned the use of the third party doctrine in the digital age. She said "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[5] This has great implications for the use of drones to monitor, collect, and store information that can then be shared with the Government under an outdated third party doctrine.

As all states can do, some states have provided greater protection than what the federal Constitution affords to third party records. Such protections may be found in legislation, court cases, or even state constitutions. Each individual state should be familiar with its own laws on third party records in determining whether or not such a provision needs to be included in that state's drone legislation.

Conclusion

NACDL encourages the implementation of the above suggestions into model legislation regulating the use of domestic drones. We look forward to working with you. Please contact NACDL's National Security and Privacy Counsel, Mason Clutter, with any questions. She may be reached at mclutter@nacdl.org or 202-465-7658.

---

[4] United States v. Jones, 132 S.Ct. 945 (2012) ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'. . . The Government physically occupied private property for the purpose of obtaining information.).

[5] *Id*. at 10.

113TH CONGRESS
1ST SESSION

BILL NUMBER

[Purpose]: To protect individual privacy against unwarranted governmental intrusion through the use of unmanned aerial systems commonly called drones, and for other purposes.

IN THE [CHAMBER] OF THE UNITED STATES

DATE
Xx introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To protect individual privacy against unwarranted governmental intrusion through the use of unmanned aerial systems commonly called drones, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "[Insert Short Title"]

SECTION 2. DEFINITIONS.

In this Act---

(a) the term "unmanned aircraft" means any aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (as defined in section 331 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note). and
(b) the term "law enforcement agency" means a person or entity authorized by law, or funded by the Government of the United States, to investigate or prosecute offenses against the United States.
(c) the term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.

(d) the term "anti-personnel device" means any projectile, chemical substance, electrical or directed-energy emission, whether visible or invisible, designed to harm, incapacitate, or otherwise negatively impact a human being.

SEC. 3. PROHIBITED USE OF UNMANNED AIRCRAFT SYSTEMS

Except as provided in section 4, a person or entity acting under the authority, or funded in whole or in part by, the Government of the United States shall not use an unmanned aircraft for surveillance of a person within the United States or for the surveillance of personal or business property located within the borders of the United States to gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation except to the extent authorized in a warrant that satisfies the requirements of the Fourth Amendment to the Constitution of the United States.

SEC. 4. EXCEPTIONS

This Act does not prohibit any use of an unmanned aircraft for surveillance during the course of the following:

(a) PATROL OF NATIONAL BORDERS - The use of an unmanned aircraft to patrol within 25 miles of a national border for purposes of policing the border to prevent or deter illegal entry of any persons, illegal substances, or contraband.

(b) EXIGENT CIRCUMSTANCES - The use of an unmanned aircraft by a law enforcement agency is permitted when exigent circumstances exist. For the purposes of this paragraph, exigent circumstances exist when a law enforcement agency possesses reasonable suspicion that absent swift preventative action, there is an imminent danger to life or imminent risk of threat of bodily harm.

(c) DURING AN ENVIRONMENTAL OR WEATHER RELATED CATASTROPHE – The use of an unmanned aircraft by federal and state authorities to preserve public safety, protect property, and conduct surveillance for the assessment and evaluation of environmental or weather related damage, erosion, flood or contamination during a lawfully declared state of emergency.

SEC. 5. PROHIBITED SURVEILLANCE UNDER THIS ACT

This Act prohibits any use of an unmanned aircraft for the following:

(a) USE OF FORCE - No Federal agency may authorize the domestic use, including granting a permit for use, of an unmanned aircraft while armed with a lethal weapon or anti-personnel device.

(b) DOMESTIC USE IN PRIVATE SURVEILLANCE - No Federal agency may authorize the domestic use, including granting a permit for use, of an unmanned aircraft

to permit any private person to conduct surveillance upon any other private person without the express, informed consent of the private person or persons to be made subject to surveillance, or the owner or lessee of any real property on which that other private person is present.

(c) SURVEILLANCE OF THE EXERCISE OF 1ST AMMENDMENT RIGHTS - No Federal agency may authorize the domestic use, including granting a permit for use, of an unmanned aircraft for the purpose of the surveillance of persons engaged in the lawful exercise of First Amendment rights and or the Right of Freedom of Assembly.

SEC. 6. REMEDIES FOR VIOLATION.

Any aggrieved party may in a civil action obtain all appropriate relief to prevent or remedy a violation of this Act.

SEC. 7. PROHIBITIONS ON THE CONDUCT OF UNMANNED AIRCRAFT SURVEILLANCE AND THE USE OF ACQUIRED SURVEILLANCE AS EVIDENCE.

This Act prohibits the following:

(a) No evidence obtained or collected in violation of this Act may be admissible as evidence in a criminal prosecution during trial, at sentencing, before a grand jury, as rebuttal evidence, or during administrative hearings in any court of law in the United States.

(b) No imaging or other forms of observational data gathered by unmanned aircraft surveillance from or concerning the parties or places subjected to surveillance in violation of this Act may be preserved by law enforcement or government agencies for any purpose unless required by a Federal Court.

(c) No imaging or any other forms of data lawfully obtained under this Act for which there is not a reasonable and articulable suspicion that such images or data contain evidence of a crime, or are relevant to an ongoing investigation or trial, may be retained for more than 90 days, unless such retention is attendant to general agency guidelines regarding the retention of evidence in criminal cases. In such cases, the imaging or other data may not be distributed to agencies, entities, or individuals where such distribution is not necessary to meet general agency guidelines regarding the retention of evidence in criminal cases. A court order must be obtained before imaging or other forms of data may be retained lawfully for more than 90 days.

(d) No unmanned aircraft may conduct any type of surveillance that would violate Federal laws regarding the interception of aural communications, electronic communications and transmissions, personal location data, or the acquisition of video or still images of a person or conditions existing within a home or place without first obtaining all required warrants in compliance with the Federal or state statutes applying to such interceptions.

SEC. 8. DOCUMENTATION OF DRONE SURVEILLANCE

(a) All use of unmanned aircraft for surveillance shall be documented by the person or entity authorized to conduct the surveillance. All surveillance flights shall be documented as to:

(i) duration, flight path;
(ii) mission objectives, and
(iii) the names of places or persons authorized to be subject to surveillance.

(b) This flight information noted will be certified as accurate and complete by the supervising person authorized by a court to conduct the surveillance.

(c) This flight information must be retained for a period of five years.

(d) Persons seeking relief before a court of law or an administrative agency who have been a target of unmanned aircraft surveillance may obtain by proper motion to the court all information relating to them acquired in the course of such surveillance, excepting only the operational capabilities of the unmanned aircraft, unmanned aircraft system, and other operational information strictly related to the technical conduct and physical security of the surveillance operation.

EXHIBIT A

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

AVIATION COMMITTEE

Recommended Guidelines for the use of Unmanned Aircraft

BACKGROUND:

Rapid advances in technology have led to the development and increased use of unmanned aircraft. That technology is now making its way into the hands of law enforcement officers nationwide.

We also live in a culture that is extremely sensitive to the idea of preventing unnecessary government intrusion into any facet of their lives. Personal rights are cherished and legally protected by the Constitution. Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety. From enhanced officer safety by exposing unseen dangers, to finding those most vulnerable who may have wandered away from their caregivers, the potential benefits are irrefutable. However, privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UA by their police.

The Aviation Committee has been involved in the development of unmanned aircraft policy and regulations for several years. The Committee recommends the following guidelines for use by any law enforcement agency contemplating the use of unmanned aircraft.

DEFINITIONS:

1. **Model Aircraft** - A remote controlled aircraft used by hobbyists, which is manufactured and operated for the purposes of sport, recreation and/or competition.
2. **Unmanned Aircraft (UA)** – An aircraft that is intended to navigate in the air without an on-board pilot. Also called Remote Piloted Aircraft and "drones."
3. **UAS Flight Crewmember** - A pilot, visual observer, payload operator or other person assigned duties for a UAS for the purpose of flight.
4. **Unmanned Aircraft Pilot** - A person exercising control over an unmanned aircraft during flight.

COMMUNITY ENGAGEMENT:

1. Law enforcement agencies desiring to use UA should first determine how they will use this technology, including the costs and benefits to be gained.
2. The agency should then engage their community early in the planning process, including their governing body and civil liberties advocates.
3. The agency should assure the community that it values the protections provided citizens by the U.S. Constitution. Further, the agency will operate the aircraft in full compliance with the mandates of the Constitution, federal, state and local law governing search and seizure.
4. The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy.
5. As with the community, the news media should be brought into the process early in its development.

SYSTEM REQUIREMENTS:

1. The UAS should have the ability to capture flight time by individual flight and cumulative over a period of time. The ability to reset the flight time counter should be restricted to a supervisor or administrator.
2. The aircraft itself should be painted in a high visibility paint scheme. This will facilitate line of sight control by the aircraft pilot and allow persons on the ground to monitor the location of the aircraft. This recommendation recognizes that in some cases where officer safety is a concern, such as high risk warrant service, high visibility may not be optimal. However, most situations of this type are conducted covertly and at night. Further, given the ability to observe a large area from an aerial vantage point, it may not be necessary to fly the aircraft directly over the target location.
3. Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program.

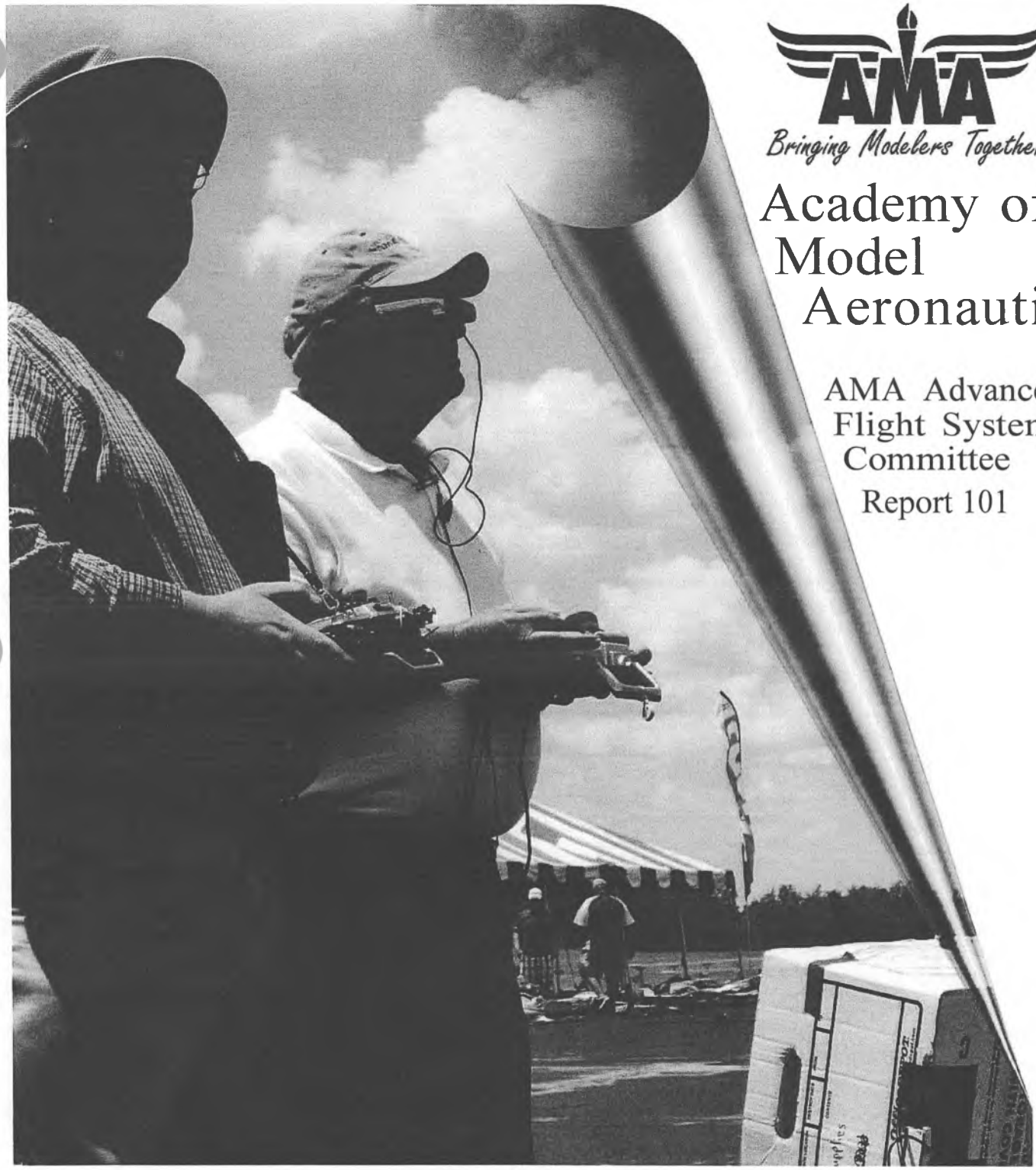
4. The use of model aircraft, modified with cameras, or other sensors, is discouraged due to concerns over reliability and safety.

OPERATIONAL PROCEDURES:

1. UA operations require a Certificate of Authorization (CAO) from the Federal Aviation Administration (FAA). A law enforcement agency contemplating the use of UA should contact the FAA early in the planning process to determine the requirements for obtaining a COA.
2. UAS will only be operated by personnel, both pilots and crew members, who have been trained and certified in the operation of the system. All agency personnel with UA responsibilities, including command officers, will be provided training in the policies and procedures governing their use.
3. All flights will be approved by a supervisor director's office and must be for a legitimate public safety mission, training, or demonstration purposes.
4. All flights will be documented on a form designed for that purpose and all flight time shall be accounted for on the form. The reason for the flight and name of the supervisor approving will also be documented.
5. An authorized supervisor/administrator will audit flight documentation at regular intervals. The results of the audit will be documented. Any changes to the flight time counter will be documented.
6. Unauthorized use of a UA will result in strict accountability.
7. Except for those instances where officer safety could be jeopardized, the agency should consider using a "Reverse 911" telephone system to alert those living and working in the vicinity of aircraft operations (if such a system is available). If such a system is not available, the use of patrol car public address systems should be considered. This will not only provide a level of safety should the aircraft make an uncontrolled landing, but citizens may also be able to assist with the incident.
8. Where there are specific and articulable grounds to believe that the UA will collect evidence of criminal wrongdoing and if the UA will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight.

IMAGE RETENTION:

1. Unless required as evidence of a crime, as part of an on-going investigation, for training, or required by law, images captured by a UA should not be retained by the agency.
2. Unless exempt by law, retained images should be open for public inspection.



Bringing Modelers Together

Academy of Model Aeronautics

AMA Advanced Flight Systems Committee

Report 101

AMA Policies for Radio Controlled Model Aircraft Operations Utilizing First Person View, Failsafe, Stabilization and Autopilot Systems

(Revision 07/20/2013)

Academy of Model Aeronautics
"AMA Advanced Flight Systems Committee"
amaflightsystems@gmail.com

October 21, 2012
RE: AMA Flight Systems Policies
AMA Documents #550 and #560

Greetings,

In June of 2012 the AMA Advanced Flight Systems Committee (AFSC) was created for the purpose of developing operational policies and guidelines for advanced flight systems used in radio controlled model aircraft.

The committee's first project was to evaluate and revise AMA's current policies for *"R/C Model Aircraft Operations Utilizing First Person View Systems"* (AMA Document #550) and *"R/C Model Aircraft Operations Utilizing Failsafe, Stabilization & Autopilot Systems"* (AMA Document #560).

The committee in a collaborative effort with leading members of the hobby industry and FPV community revised these documents and presented this report to the Executive Council during the October 20, 2012 council meeting. Revisions were made and the report and documents were adopted by the council.

As new aeromodeling technologies emerge the AFSC will develop and/or revise AMA operational documents/policies. A footer to each document page contains the latest revision date.

Thank you,

Bob Brown
AMA President

Academy of Model Aeronautics
AMA Advanced Flight Systems Committee
amaflightsystems@gmail.com

Radio Controlled Model Aircraft Operations
AMA Documents #550 and #560

Additional Updates of AMA Flight System Documents #550 and #560:

The AMA posted on the AMA website its revised policies for R/C model aircraft operations utilizing First Person View (FPV) systems (AMA document # 550) and Failsafe, Stabilization and Autopilot Systems (AMA document #560) on November 2, 2012.

After a two month review by aeromodeling stakeholders, including members of the AMA and FPV community, the AMA Advanced Flight Systems Committee responded to questions for additional clarification for some operational statements within the documents. As a result of this collaboration several items within AMA documents #550 and #560 were revised on 01/14/2013 and the updated documents have been posted in the AMA website Document section titled "Advanced Flight Systems".

The committee appreciates those FPV enthusiasts and stakeholders who offered suggestions for operational changes to enhance the documents and improve clarity.

The AMA recognizes the importance of providing relevant and up-to-date operational policies and guidelines enabling members to utilize and participate in new aeromodeling technologies and disciplines. The AFS committee welcomes continued collaboration with aeromodeling stakeholders in efforts to improve the quality of AMA's safety programing.

Andy Argenio
AMA Chairman
Advanced Flight Systems Committee
amaflightsystems@gmail.com

Table of Contents

Introduction – Background, Consideration and Membership Education 1-2

Radio Controlled Model Aircraft Operation Utilizing "First Person View" Systems AMA Document 550

Radio Controlled Model Aircraft Operation Utilizing Failsafe, Stabilization and Autopilot Systems AMA Document 560

Frequently Asked Questions

Department of Transportation Federal Aviation Administration 14 CFR Part 91
Docket No. FAA-2006-25714
Unmanned Aircraft Operations in the National Airspace System

FAA Modernization and Reform Act of 2012

Academy of Model Aeronautics
"AMA Advanced Flight Systems Committee"
amaflightsystems@gmail.com

Introduction
Radio Controlled Model Aircraft Operations
Utilizing First Person View, Failsafe, Stabilization and Autopilot Systems

1. Background:

AMA created its "*First Person View*" (FPV) policy (*AMA Document #550*) in 2008 *and "Manually Controllable Programed Outdoor Model Flight Operations"* policy (*AMA Document #560*) in 2011. These policies were adopted to provide operational guidelines for AMA members that would enable them to participate in these disciplines within the parameters of AMA's safety programming.

In recent years FPV, stabilization, and autopilot systems have become more reliable and safer for flying model aircraft. Advancements in technology, as well as the increased number of people participating in FPV flying prompted AMA members and nonmembers to request a review of documents #550 and #560 to consider revisions that would relax some requirements.

In June of 2012, AMA President Bob Brown established an AMA committee to evaluate and revise AMA's current policy documents #550 and #560. Subsequently, a decision was made to broaden the objectives of the committee to evaluate and/or develop policies for any new aeromodeling technologies resulting in the following committee name and mission.

Advanced Flight Systems Committee (AFSC)
amaflightsystems@gmail.com

Mission Statement: "*To analyze advanced flight systems for the purpose of developing program-specific operational requirements, procedures, guidelines, and recommendations to ensure compliance with or updating of AMA's National Model Aircraft Safety Code.*"

Committee members were chosen because of their knowledge and expertise of the AMA National Safety Code and Insurance program, FAA and Government Relations, Public Relations, Unmanned Aerial Systems, and/or Engineering/Technology.
Chairman: Andy Argenio
Committee Members: Bob Brown, Dave Mathewson, Rich Hanson, Jim Rice, Lawrence Tougas, and Chris Brooks.

The committee's objectives are to develop operational procedures for advanced model aircraft flight systems and to ensure AMA safety standards are maintained when embracing new technologies.

2. Considerations:

In the process of revising #550 and #560, the committee considered input from members including comments made in a petition from the FPV community sent to AMA leadership. Policy decisions had to comply with or address the requirements, issues, concerns and suggestions from the following documents, laws, members and membership groups:

- AMA's National Model Aircraft Safety Code
- Federal Bill H.R. 658/Public Law 112-95
- AMA's Liability Insurance Program • Existing Aeromodeling Disciplines
- FPV Community and AMA Members

A review/comparison was done of other aeromodeling association's FPV policies. It included Model Aeronautics Association of Canada (MAAC), British Model Flying Association (BMFA), and Model Aeronautical Association of Australia (MAAA) and revealed that all required a spotter for the FPV pilot, range of flights were limited by law to VLOS, and buddy boxes were required at all times.

3. Membership Education:

The committee recognized a need to educate members on FPV and autopilot system by including in the revised documents a section for definitions, recommendations, and general information. Members often times mistakenly associate FPV and autopilot activities with their knowledge of drones. AMA modelers are not building or purchasing UAVs or drones whose flights are mission oriented, or flown beyond VLOS, or computer controlled for nearly their entire flight. AMA members are attracted to the recreational visual experience of FPV flying and the use of stabilization and autopilot systems to improve flight performance.

Without a basic understanding of these systems and AMA's rules for implementation and operation, erroneous assumptions have been made that these systems present a greater risk for model aircraft accidents/incidents and the AMA should exclude these types of operations for AMA members. The fact is stabilization and autopilot systems in model aircraft have the capability to reduce the risk and severity of model aircraft accidents. Several examples follow:

- AMA FPV flying involves two persons, a pilot and spotter, providing a higher level of situational awareness surrounding the model aircraft to identify and prevent conflicts or collisions.
- R/C Pilots have direct transmitter control to activate or deactivate programmable autopilot systems to recover an out of control model aircraft to level flight, maintain a heading, return an aircraft to a selected location, or initiate a programmed flight path.
- Autopilot systems may be programmed to prevent a flyaway by safely returning a model aircraft to a selected safe location when a radio link is lost.

Radio Controlled Model Aircraft Operation Utilizing "First Person View" Systems

1. DEFINITION OF TERMS:

Please refer to Page 5 section 7 which contains an alphabetical listing of the definitions of the terms in italics that are used in this document.

2. GENERAL:

FPV flying of radio control model aircraft by AMA members is allowed only for noncommercial purposes as a hobby/recreational and/or competition activity and must be conducted in accordance with AMA's current National Model Aircraft Safety Code and any additional rules specific to a flying site/location.

3. OPERATIONS – REQUIREMENTS – LIMITATIONS:

a) AMA *FPV novice pilots* must use a buddy-box system with an *FPV spotter* while learning to fly *FPV*.

b) All *FPV* flights require an AMA *FPV pilot* to have an AMA *FPV spotter* next to him/her maintaining *VLOS* with the *FPV aircraft* throughout its flight.

c) The *FPV pilot* must brief the *FPV spotter* on the *FPV spotter's* duties, communications and hand-over control procedures before *FPV flight*.

d) The AMA *FPV spotter* must communicate with the *FPV pilot* to ensure the *FPV aircraft* remains within *VLOS*, warning the *FPV pilot* of approaching aircraft, and when avoidance techniques are necessary.

e) During an FPV flight, the FPV spotter must be prepared to acquire the transmitter/control from the *FPV pilot* and assume *VLOS* control of the model aircraft at any time safe operation of the flight is in question.

f) If the *FPV pilot* experiences a problem due to a loss of video link, orientation, or is unable to safely fly, he/she must abandon *FPV* mode and fly *VLOS* or pass the RC transmitter to the *FPV spotter* to assume *VLOS* control of the model aircraft.

g) Before the initial *FPV* flight of an *FPV model aircraft* and/or after any changes or repairs *to essential flight systems*, the *FPV model aircraft* must have an *R/C test flight* by conventional *VLOS*.

h) *FPV model aircraft* must use frequencies approved by the FCC for both the RC system and the wireless video system. Pilots must meet applicable FCC licensing requirements if they choose to operate the RC flight control system or the wireless video system on Amateur Band frequencies.

4. RANGE – ALTITUDE – WEIGHT – SPEED:

a) One of the requirements in Federal Law (Public Law 112-95 Sec 336 (c) (2) February 14, 2012) for model aircraft to be excluded from FAA regulations is that model aircraft must be flown within *VLOS* of the operator.

b) Model aircraft flown using *FPV* must remain at or below 400 feet AGL when within 3 miles of an airport as specified in the AMA Safety Code.

c) Model aircraft flown *FPV* are limited to a weight (including fuel, batteries, and onboard *FPV* equipment) of 15lbs. and a speed of 70mph.

5. RECOMMENDATIONS & INFORMATION:

a) AMA *FPV novice pilots* should consider using a cockpit view flight simulator to become accustomed to *FPV* flight.

b) AMA *FPV pilots* should consider using a programmable *autopilot* (AMA Document #560) with a failsafe "return to launch" (RTL) feature that will maintain control of the aircraft in the event of signal loss.

c) An onboard camera equipped with a pan and tilt mount that is positioned by head tracking goggles, will improve the *FPV pilot's* situational awareness of airspace surrounding the *FPV aircraft* during flight, but does not replace the requirement for an AMA *FPV spotter.*

d) When purchasing *FPV* operational systems, always try to select quality equipment, verify its compatibility, install components for interference rejection, and determine that signal range is adequate for maximum VLOS range.

6. PRIVACY PROTECTION SAFEGUARDS:

The use of imaging technology for aerial surveillance with radio control model aircraft having the capability of obtaining high-resolution photographs and/or video, or using any types of sensors, for the collection, retention, or dissemination of surveillance data information on individuals, homes, businesses, or property at locations where there is a reasonable expectation of privacy is strictly prohibited by the AMA unless written expressed permission is obtained from the individual property owners or managers.

7. DEFINITIONS OF TERMS:

AMA FPV Pilot is an AMA member who is capable of maintaining stable flight of a model aircraft within its intended flight envelope when flown FPV without losing control or having a collision.

Buddy-Box System is a system that has one transmitter operating as the master controller, while a second transmitter is linked/slaved to it allowing dual control of an aircraft. The operator of the master transmitter allows one or the other transmitter to control the aircraft through the use of a spring-loaded switch. The switch provides instantaneous transfer of control from one transmitter to the other. The buddy-box system is an efficient and effective means of achievinga position transfer of control from one pilot to another. Although this system is commonly used for training novice fliers, it is also useful in

situations where an experienced pilot may have an increased likelihood of needing a second pilot's assistance in maintaining control of the aircraft. The use of the buddy-box may be helpful in assisting pilots with physical limitations, flying in congested environments, during times of reduced visibility, or anytime during FPV when a timely transfer of control may be beneficial.

Essential Flight Systems are any systems or components necessary to maintain stable flight within a model aircraft's flight envelope. (This includes primary radio control systems and any stabilization or gyros required to maintain stability and heading in certain types of model aircraft that would be uncontrollable/unstable without their use).

First Person View (FPV) refers to the operation of a radio controlled (R/C) model aircraft using an onboard camera's cockpit view to orient and control the aircraft.

Flight Envelope is defined as the range of airspeeds, attitudes, and flight maneuvers which a model aircraft can safely perform/operate for its intended use.

FPV Aircraft is an RC model aircraft equipped with a video transmitter to send real-time video images from an onboard camera to a ground based receiver for display on a pilot's video monitor/goggles. (*FPV model aircraft* types include: Fixed Wing, Rotary Wing, and Multi-Rotor Platforms).

FPV Novice Pilot is an AMA member learning to fly *FPV* utilizing a buddy-box system with an experienced AMA *RC pilot* operating the master transmitter and serving as the *FPV spotter*.

FPV Spotter is an experienced AMA *RC pilot* who has been briefed by the *FPV pilot* on the tasks, responsibilities and procedures involved in being a spotter; is capable and mature enough to perform the duties and is able to assume conventional *VLOS* control of the aircraft.

Non-Essential Flight Systems are any systems or components that are not necessary to maintain stable flight within the model aircraft's *flight envelope*. (This includes *autopilot* or *stabilization systems* that can be activated and deactivated in flight by the pilot without affecting stable flight).

R/C Test Flight requires an *AMA Pilot* to manually operate an R/C transmitter to control a model aircraft's flight path and determine if the aircraft is capable of maintaining stable flight within its *flight envelope*.

Visual Line Of Sight (VLOS) is the distance at which the pilot is able to maintain visual contact with the aircraft and determine its orientation without enhancements other than corrective lenses.

Academy of Model Aeronautics
AMA Advanced Flight Systems Committee
amaflightsystems@gmail.com

Radio Controlled Model Aircraft Operation Utilizing Failsafe, Stabilization and Autopilot Systems

1. DEFINITION OF TERMS:

Please refer to Page 8 section 7 which contains an alphabetical listing of the definitions of the terms in italics that are used in this document.

2. GENERAL:

All model aircraft flights utilizing *stabilization* and *autopilot* control systems must be conducted in accordance with AMA's current National Model Aircraft Safety Code and any additional rules specific to a flying site/location.

3. OPERATIONS – REQUIREMENTS – LIMITATIONS:

a) AMA members flying radio controlled model aircraft equipped with flight *stabilization* and *autopilot* systems must maintain *VLOS* with the aircraft at all times including programmed autopilot waypoint flight.

b) *AMA Pilots* must be able to instantaneously deactivate programmed flight of *autopilot systems* at any time during flight and resume manual control of the model aircraft.

c) *AMA Pilots* must perform an *R/C Test Flight* of a model aircraft before activating a newly installed *autopilot* or *stabilization system* and/or after any repairs or replacement of model aircraft *essential flight systems*.

d) Model aircraft exceeding 15lbs and/or 70mph may only use an *autopilot* for a programmed "return to launch" (RTL) flight and not for programmed waypoint flying of a predetermined course.

e) STABILIZATION & AUTOPILOT SYSTEMS MAY BE USED FOR/TO:

- Stabilization/automatically stabilize aircraft to level flight when control sticks are centered.
- Recovery/activate TRX switch to recover an out of control aircraft to level flight.
- Heading/activate TRX switch to hold a model aircraft's heading for precision flight path.
- Altitude/activate TRX switch to maintain fixed aircraft altitude while allowing directional control.
- Return GPS/activate TRX switch to return aircraft via GPS to launch point.
- Return FSS/failsafe activated from radio signal loss to return aircraft via GPS to launch point.
- Fixed circle/activate TRX switch to circle aircraft at point of activation at fixed altitude.
- Waypoint/activate TRX switch to initiate an autopilot programmed flight path via waypoints.
- Fencing/autopilot programed to display site unique boundaries on video monitor/goggles.

4. RANGE – ALTITUDE – WEIGHT – SPEED:

a) One of the requirements in Federal Law (Public Law 112-95 Sec 336 (c) (2) February 14, 2012) for model aircraft to be excluded from FAA regulations is that model aircraft be flown within *VLOS* of the operator.

b) Model aircraft must be flown at or below 400 feet AGL when within 3 miles of an airport as stated in the AMA Safety Code.

c) Model aircraft utilizing an *autopilot* for waypoint flying are limited to a maximum weight (including fuel, batteries, and onboard *autopilot systems*) of 15lbs and a speed of 70mph.

5. RECOMMENDATIONS & INFORMATION:

a) If your radio system lacks *failsafe* capability, consider using programmable digital servos or auxiliary *failsafe* modules. In the event of a radio signal failure these components will activate desired safe servo settings or an *autopilot* for return to base/launch (RTL).

b) When using an *autopilot system* the "return to launch" (RTL) feature should be programmed to return the aircraft to a safe location and safely terminate the flight should manual control of the aircraft be lost. When using RTL, pay particular attention to the manufacturer's throttle recommendations to prevent stalling.

c) The use of *stabilization systems* is recommended when flying FPV to improve flight stability and video quality.

d) Pilots usually choose to incorporate *stabilization* and *autopilot systems* for model aircraft flying to enhance flight performance, correct bad tendencies of the model aircraft, maintain stability in windy weather, establish precision heading holds for takeoffs/landings, flight training for novice pilots, create a steady flight platform for cameras, and generally just to make an airplane easier and safer to fly.

e) When purchasing *stabilization* and *autopilot systems*, always try to select quality equipment from reputable dealers, ensure for compatibility with other onboard systems, and install components according to manufacturers' instructions.

6. PRIVACY PROTECTION SAFEGUARDS:

The use of imaging technology for aerial surveillance with radio control model aircraft having the capability of obtaining high-resolution photographs and/or video, or using any types of sensors, for the collection, retention, or dissemination of surveillance data or information on individuals, homes, businesses, or property at locations where there is a reasonable expectation of privacy is strictly prohibited by the AMA unless written expressed permission is obtained from the individual property owners or managers.

7. DEFINITIONS OF TERMS:

AMA Pilot is an AMA member who is capable of manually operating an R/C transmitter to control a model aircraft's flight path within its safe intended *flight envelope* without losing control or having a collision.

Autopilot Systems incorporate programmable flight *stabilization* with an altitude sensor and a GPS receiver for accurate positioning and to navigate/control a radio controlled model aircraft's flight path. Advanced systems offer software for entering navigable waypoints. The flight data waypoints may be saved to autopilot's/GPS memory for programmed flight.

Essential Flight Systems are any systems or components necessary to maintain stable flight within a model aircraft's *flight envelope*. (This includes primary R/C systems and any *stabilization* or gyros required to maintain stability and heading in certain types of model aircraft that would be uncontrollable/unstable without their use).

Failsafe Systems are designed to minimize or prevent damage and safely terminate a flight when a radio controlled model aircraft loses radio signal. Modern radio systems can be programmed to position servos to a desired control setting in the event of radio signal failure.

First Person View (FPV) refers to the operation of a radio controlled (R/C) model aircraft using an onboard camera's cockpit view to orient and control the aircraft. (AMA Document #550).

Flight Envelope is defined as the range of airspeeds, attitudes and flight maneuvers which a model aircraft can safely perform/operate for its intended use.

Non-Essential Flight Systems are any systems or components that are not necessary to maintain stable flight within the model aircraft's intended flight envelope. (This includes *autopilot* or *stabilization systems* that can be activated and deactivated in flight by the pilot without affecting manually controlled stable flight).

R/C Test Flight requires an AMA Pilot to manually operate an R/C transmitter to control a model aircraft's flight path and determine if the aircraft is capable of maintaining stable flight within its safe intended *flight envelope*.

Stabilization Systems are designed to maintain intended model aircraft flight attitudes. The pilot can install, program and/or activate a system to stabilize yaw, pitch, or roll or any one attitude or combination of attitudes. Systems are often based on rate/heading hold gyros or inertial motion sensors utilizing multi-axis gyros and accelerometers for attitude stabilization.

Visual Line of Sight (VLOS) is the distance at which the pilot is able to maintain visual contact with the aircraft and determine its orientation and attitude without enhancements other than corrective lenses.

FREQUENTLY ASKED QUESTIONS

Model Aircraft Radio Control Operations Utilizing FIRST PERSON VIEW, STABILIZATION, AND AUTOPILOT SYSTEMS

1. **I thought it was AMA's policy to stay clear of Drone type flying using programmed flight control systems?**

   There are distinct differences between R/C FPV autopilot equipped model aircraft flying and Drone flying. Drone flights are mission oriented, flown beyond VLOS, and computer controlled for nearly their entire flight. AMA members fly R/C FPV autopilot equipped model aircraft as a recreational visual/video experience. The AMA FPV pilot is required to fly within VLOS and manually controls the aircraft via R/C for nearly the entire flight.

2. **Why has AMA chosen to limit FPV flying to VLOS when it is not currently required in the law?**

   Section 4-a of AMA document 550 and 560 states that one of the requirements in Federal Law (Public Law 112-95 Sec 336 (c) (2) February 14, 2012) for model aircraft to be excluded from FAA regulations is that model aircraft be flown within VLOS of the operator. The AMA has chosen the exclusionary path to protect and advocate for the interest of its members rather than be subject to potentially onerous governmental regulations.

3. **Will AMA pilots flying FPV beyond VLOS be covered by AMA liability insurance?**

   Coverage under the policy will be determined by the specific facts and details relating to the claim. As intentionally flying FPV aircraft beyond VLOS of the operator violates AMA Safety Code and documents 550 and 560, the AMA pilot should not rely on AMA insurance for coverage.

4. **Why were weight and speed limits set at 15lbs and 70mph for FPV flying or when using an autopilot for waypoint flying?**

   FPV aircraft speed limits were set lower than other R/C model aircraft to allow for easier visual tracking of model aircraft by the FPV Spotter and to provide extra time for the FPV Pilot to handover a transmitter to the FPV Spotter in the event of an approaching aircraft or incident.

   Model aircraft weight while flying FPV and/or the use of autopilot systems for waypoint flying was limited to 15lbs to reduce the potential or perception that someone could use these types of aircraft to carry a destructive payload beyond VLOS. Flying model aircraft while using stabilization and/or failsafe systems and/or activating an autopilot system for return to launch does not limit the aircraft to a weight of 15lbs.

5. **Why did the AMA decide to eliminate the buddy-box requirement for FPV flying**?

   The FPV Pilot is often more experienced and able to maneuver his FPV aircraft out of problem status with verbal cues from the FPV Spotter rather than having the FPV Spotter take over control using a buddy-box. The FPV Pilot will know when the video link is lost before the FPV Spotter and will hand over the transmitter to the FPV Spotter. The cost and availability of compatible and programmable radiotransmitters for use as a buddy-box for complex FPV aircraft systems may also preclude the use of a buddy-box. It is also possible that some of the more complex systems might require the buddy box port for flight/camera operations.

6. **Does the FPV Spotter need to be an experienced FPV Pilot?**

   The FPV Spotter is required to be an experienced R/C Pilot but doesn't need to be an experienced FPV Pilot since he will only be required to fly the FPV Aircraft by conventional VLOS in the event of an incident.

7. **When will an FPV Novice Pilot assume FPV Pilot status?**

   When an FPV Novice Pilot is able to consistently maintain control of stability and orientation while flying an FPV aircraft, without losing control or having a collision, he/she may assume FPV Pilot status. The buddy-box is no longer required for FPV Pilots.

8. **Will my AMA club have to allow FPV flying at the club's AMA chartered club field?**

   Each AMA club and/or site owner or property manager decides what can or cannot be flown at a particular flying site.

9. **I have heard that FPV flying and the use of complex autopilot systems will create a much greater risk of accidents occurring at my club's flying site. If this is true, shouldn't the AMA exclude FPV and Autopilot flying at all AMA chartered flying sites?**

   Educating members so they understand the basics of these systems and AMA's requirements for use and implementation should alleviate these erroneous assumptions. The fact is FPV flying and the use of Stabilization and Autopilot systems in model aircraft have the capability to reduce the risk and severity of model aircraft accidents.

10. **Was there any consideration given to having a proficiency system for FPV Pilots similar to what jet pilots have to undergo?**

    When necessary, as with high energy and high risk turbine powered aircraft, pilot testing was implemented into our safety programming to mitigate the risks involved. The committee felt that requiring a Spotter for FPV and providing a transmitter hand-over protocol for FPV Pilots and a buddy-box for novice pilots, would ensure AMA Safety Standards were maintained.

11. **Who qualifies AMA FPV Pilots?**

    Except for AMA members piloting turbine powered model aircraft, the AMA doesn't require pilot proficiency testing. Individual AMA Clubs may establish their own pilot testing requirements for their members which may require the members to demonstrate and be judged on their flying proficiency. The AMA does expect members to use their good judgment to decide for themselves whether or not they can fly a model aircraft safely. With regard to FPV flying this would be when the AMA FPV Novice Pilot was satisfied that he/she was capable of maintaining control of stability and orientation of FPV model aircraft when flown FPV without losing control or having a collision. The FPV novice pilot would now have AMA FPV Pilot status.

12. **Will elimination of the buddy-box requirement and hand-over control to the FPV Spotter create a greater risk of accidents?**

We discovered in our observations that FPV flying for the most part took place at either higher altitudes or lower "near ground" altitudes then typical model aircraft flying. Hand-over transferring of the transmitter from the FPV Pilot to the Spotter provided sufficient time for recovery at the higher altitudes. Transference via the buddy-box for an out of control FPV aircraft at the lower altitudes didn't provide a better chance of preventing a crash than handing over control to the spotter. Both methods proved inadequate at these near ground or lower altitudes.

13. **Are AMA members covered by AMA insurance when their model aircraft's FPV flight goes beyond the AMA chartered club's flying site boundaries?**

AMA insurance liability protection is not limited to AMA charted club flying sites or the flight boundaries of the site. It applies to accidents arising from AMA member modeling activities of model aircraft conducted in accordance with AMA's National Safety Code. As long as AMA pilots don't fly at locations where model airplane flying is prohibited and avoid flying directly over unprotected people, vessels, vehicles or structures and avoid endangering life or property, AMA insurance coverage will be extended. This coverage also extends to an accidental model aircraft fly-away beyond the permitted flying site that may cause bodily injury or property damage at any location where the crash occurs.

14. **Can FPV model aircraft be flown by AMA members at altitudes above 400' and is there any chance that we might someday be able to fly beyond VLOS?**

In 1981 FAA Advisory Circular AC 91-57 advised that model aircraft not exceed altitudes of 400ft. At this time there is no FAA regulation/rule preventing model aircraft from flying above 400' AGL. For the past 32 years the AMA applied this FAA advisory only within 3 miles of an airport in the AMA National Safety Code. The AMA will continue to use all its resources to prevent the FAA from making 400' a regulation/rule for all locations of model aircraft flying. Public Law 112-95 Sec 336 requires model aircraft be flown within VLOS. As you might expect this is acceptable by the majority of AMA members but limiting to FPV activity. We are looking into alternative methods to support FPV activity beyond VLOS as new FPV technology (perhaps sense and avoid) becomes available and risks assessed and mitigated to a safe and acceptable level to perhaps someday fly beyond VLOS.

15. **Why were privacy protection requirements included in the revised documents?**

These safeguards were included to provide 4th Amendment rights to privacy protection for individuals and their property from model aircraft equipped with imaging technology ***when used for surveillance.*** *One of the provisions in Federal Law 112-95 Sec 336-2 for model aircraft to be excluded from FAA regulations requires model aircraft are operated within the programming of a nationwide community-based organization (CBO) that has been accepted/approved for CBO status by the FAA. The AMA has chosen this path in order to operate under its accepted Safety Code and Operational Requirements including Privacy Protection Safeguards rather than be subject to potentially onerous governmental regulations with respect to Privacy Protection for those operating model aircraft outside of the CBO default path. We also had a responsibility to provide operational standards that are acceptable and compliant within our insurance programming, requiring members to operate their model aircraft without violating existing laws which could include first and fourth amendment rights of citizens to privacy protection in cases where a suit is filed for invasion of privacy as a result of unauthorized aerial surveillance.*

16. Does the AMA Privacy Protection Statement essential outlaw aerial photography and videoing?

The AFS committee views the updated AMA Privacy Protection Statement as not at all outlawing aerial photographing or videoing. We believe it's better for us to have written our own Privacy Protection Safeguard then leave it unattended; waiting for what very well may be onerous government privacy regulation. In the US anyone may take photos/videos in public places except when a legal statute or ordinance exist and when individuals are in places where they have a reasonable expectation of privacy such as restrooms, dressing rooms, medical facilities and inside their homes. Property owners may legally prohibit video/photography on their premises but have no right to prohibit others from videoing/photographing their property from other locations (which may include from airspace near their property or 400' above their property without the use of telephoto lenses while not flying directly over people or structures). In most locations you may reasonably assume that taking video/photographs is allowed and that you do not need explicit permission. However, this is a judgment call and you should request permission when the circumstances suggest that the owner is likely to object. Taking aerial photos/videos that include a person's house and property may be fine but doing so in the fenced in pool area when someone is skinny dipping would not be permissible.

[4910-13] DEPARTMENT OF TRANSPORTATION
Federal Aviation Administration
14 CFR Part 91
Docket No. FAA-2006-25714

Unmanned Aircraft Operations in the National Airspace System
AGENCY: Federal Aviation Administration (FAA), DOT.
ACTION: Notice of policy; opportunity for feedback.
SUMMARY: This notice clarifies the FAA's current policy concerning operations of unmanned aircraft in the National Airspace System.

FOR FURTHER INFORMATION CONTACT: Kenneth D. Davis, Manager, Unmanned Aircraft Program Office, Aircraft Certification Service, Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591, (202) 385-4636, email: kenneth.d.davis@faa.gov.

Background

Simply stated, an unmanned aircraft is a device that is used, or is intended to be used, for flight in the air with no onboard pilot. These devices may be as simple as a remotely controlled model aircraft used for recreational purposes or as complex as surveillance aircraft flying over hostile areas in warfare. They may be controlled either manually or through an autopilot using a data link to connect the pilot to their aircraft. They may perform a variety of public services: surveillance, collection of air samples to determine levels of pollution, or rescue and recovery missions in crisis situations. They range in size from wingspans of six inches to 246 feet; and can weigh from approximately four ounces to over 25,600 pounds. The one thing they have in common is that their numbers and uses are growing dramatically. In the United States alone, approximately 50 companies, universities, and government organizations are developing and producing some 155 unmanned aircraft designs. Regulatory standards need to be developed to enable current technology for unmanned aircraft to comply with Title 14 Code of Federal Regulations (CFR). The Federal Aviation Administration's current policy is based on whether the unmanned aircraft is used as a public aircraft, civil aircraft or as a model aircraft.

Unmanned Aircraft Systems Operating as Public Aircraft

The most common public use of unmanned aircraft today in the United States is by the Department of Defense. U.S. operations in Iraq, Afghanistan and elsewhere have fueled a huge increase in unmanned aircraft demand. In Iraq alone, more than 700 unmanned aircraft are in use for surveillance and weapons delivery. Other agencies have also found public uses for unmanned aircraft. For example, the Customs and Border Protection uses them to patrol along the US/Mexican border. In the future, unmanned aircraft could be used to provide first responder reports of damage due to weather or other catastrophic causes. In response to this growing demand for public use unmanned aircraft operations, the FAA developed guidance in a Memorandum titled "Unmanned Aircraft Systems Operations in the U.S. National Airspace System – Interim Operational Approval Guidance" (UAS Policy 05-01). In this document, the FAA set out guidance for public use of unmanned aircraft by defining a process for evaluating applications for Certificate(s) of Waiver or Authorization (COA's) for unmanned aircraft to operate in the National Airspace System.

The concern was not only that unmanned aircraft operations might interfere with commercial and general aviation aircraft operations, but that they could also pose a safety problem for other airborne vehicles, and persons or property on the ground. The FAA guidance supports unmanned aircraft flight activity that can be conducted at an acceptable level of safety. In order to ensure this level of safety, the operator is required to establish the Unmanned Aircraft System's (UAS) airworthiness either from FAA certification, a DOD airworthiness statement, or by other approved means. Applicants also have to demonstrate that a collision with another aircraft or other airspace user is extremely improbable as well as complying with appropriate cloud and terrain clearances as required. Key to the concept is the roles of pilot-in-command (PIC) and observer. The PIC concept is essential to the safe operation of manned aircraft. The FAA's UAS guidance applies this PIC concept to unmanned aircraft and includes minimum qualifications and currency requirements. The PIC is simply the person in control of, and responsible for, the UAS. The role of the observer is to observe the activity of the unmanned aircraft and surrounding airspace, either through line-of-sight on the ground or in the air by means of a chase aircraft. In general, this means the pilot or observer must be, in most cases, within 1 mile laterally and 3,000 feet vertically of the unmanned aircraft. Direct communication between the PIC and the observer must be maintained at all times. Unmanned aircraft flight above 18,000 feet must be conducted under Instrument Flight Rules, on an IFR flight plan, must obtain ATC clearance, be equipped with at least a Mode C transponder (preferably Mode S), operating navigation lights and / or collision avoidance lights and maintain communication between the PIC and Air Traffic Control (ATC). Unmanned aircraft flights below 18,000 feet have similar requirements, except that if operators choose to operate on other than an IFR flight plan, they may be required to pre-coordinate with ATC.

The FAA has issued more than 50 COA's over the past 2 years and anticipates issuing a record number of COA's this year. For more information, Memorandum on UAS Policy (05-01) and other policy guidance is available at the FAA Website: http://www.faa.gov/uas.

Unmanned Aircraft Systems Operating as Civil Aircraft

Just as unmanned aircraft have a variety of uses in the public sector; their application in commercial or civil use is equally diverse. This is a quickly growing and important industry. Under FAA policy, operators who wish to fly an unmanned aircraft for civil use must obtain an FAA airworthiness certificate the same as any other type aircraft. The FAA is currently only issuing special airworthiness certificates in the experimental category. Experimental certificates are issued with accompanying operational limitations (14 CFR §91.319) that are appropriate to the applicant's operation. The FAA has issued five experimental certificates for unmanned aircraft systems for the purposes of research and development, marketing surveys, or crew training. UAS issued experimental certificates may not be used for compensation or hire. The applicable regulations for an experimental certificate are found in 14 CFR§§21.191, 21.193, and 21.195. In general, the applicant must state the intended use for the UAS and provide sufficient information to satisfy the FAA that the aircraft can be operated safely. The time or number of flights must be specified along with a description of the areas over which the aircraft would operate. The application must also include drawings or detailed photographs of the aircraft. An on-site review of the system and demonstration of the area of operation may be required. Additional information on how to apply for an experimental airworthiness certificate is available from Richard Posey, AIR-200, (202) 267-9538; email: richard.posey@faa.gov

Recreational/Sport Use of Model Airplanes

In 1981, in recognition of the safety issues raised by the operation of model aircraft, the FAA published Advisory Circular (AC) 91-57, Model Aircraft Operating Standards for the purpose of providing guidance to persons interested in flying model aircraft as a hobby or for recreational use. This guidance encourages good judgment on the part of operators so that persons on the ground or other aircraft in flight will not be endangered. The AC contains among other things, guidance for site selection. Users are advised to avoid noise sensitive areas such as parks, schools, hospitals, and churches. Hobbyists are advised not to fly in the vicinity of spectators until they are confident that the model aircraft has been flight tested and proven airworthy. Model aircraft should be flown below 400 feet above the surface to avoid other aircraft in flight. The FAA expects that hobbyists will operate these recreational model aircraft within visual line-of-sight. While the AC 91-57 was developed for model aircraft, some operators have used the AC as the basis for commercial flight operations.

Policy Statement

The current FAA policy for UAS operations is that no person may operate a UAS in the National Airspace System without specific authority. For UAS operating as public aircraft the authority is the COA, for UAS operating as civil aircraft the authority is special airworthiness certificates, and for model aircraft the authority is AC 91-57. The FAA recognizes that people and companies other than modelers might be flying UAS with the mistaken understanding that they are legally operating under the authority of AC 91-57. AC 91-57 only applies to modelers, and thus specifically excludes its use by persons or companies for business purposes. The FAA has undertaken a safety review that will examine the feasibility of creating a different category of unmanned "vehicles" that may be defined by the operator's visual line of sight and are also small and slow enough to adequately mitigate hazards to other aircraft and persons on the ground. The end product of this analysis may be a new flight authorization instrument similar to AC 91-57, but focused on operations which do not qualify as sport and recreation, but also may not require a certificate of airworthiness. They will, however, require compliance with applicable FAA regulations and guidance developed for this category. Feedback regarding current FAA policy for Unmanned Aircraft Systems can be submitted at www.faa.gov/uas. (Scroll down to the bottom of the page and find Contact UAPO. Click into this link.)

Issued in Washington, DC on February 6, 2007/s/ Nick Sabatini

Nicholas Sabatini
Associate Administrator for Aviation Safety

FAA Modernization and Reform Act of 2012

Senate Bill, Section 607(g) ...exempts most model airplanes used for recreational or academic use from any UAS regulations established by the FAA

Conference Committee Report

Senate bill with modifications... *Language including model aircraft for the purposes of sports, competitions and academic purposes is removed and replaced with ``hobby''. The modified section includes language requiring that the model aircraft must be operated in a manner that does not interfere with and gives way, to all manned aircraft. In addition, language that requires that model aircraft flown within five miles of an airport will give prior notification to the airport and the air traffic control (ATC), and that model aircraft that are flown consistently within five miles of the ATC will do so under standing agreements with the airports and ATC. Lastly, language is added that will ensure that nothing in this provision will interfere with the Administrator's authority to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system. In this section the term ``nationwide community-based organization'' is intended to mean a membership based association that represents the aeromodeling community within the United States; provides its members a comprehensive set of safety guidelines that underscores safe aeromodeling operations within the National Airspace System and the protection and safety of the general public on the ground; develops and maintains mutually supportive programming with educational institutions, government entities and other aviation associations; and acts as a liaison with government agencies as an advocate for its members.*

SEC. 336. SPECIAL RULE FOR MODEL AIRCRAFT.

(a) In General.--Notwithstanding any other provision of law relating to the incorporation of unmanned aircraft systems into Federal Aviation Administration plans and policies, including this subtitle, the Administrator of the Federal Aviation Administration may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft, if--

(1) the aircraft is flown strictly for hobby or recreational use;

(2) the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;

(3) the aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;

(4) the aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and

(5) when flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed upon operating procedure with the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport)).

(b) Statutory Construction.--Nothing in this section shall be construed to limit the authority of the Administrator to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system.

(c) Model Aircraft Defined.--In this section, the term ``model aircraft'' means an unmanned aircraft that is--

(1) capable of sustained flight in the atmosphere;

(2) flown within visual line of sight of the person operating the aircraft; and

(3) flown for hobby or recreational purposes.

Bill Text: TX HB912 | 2013-2014 | 83rd Legislature | Enrolled

Texas House Bill 912 ***(Adjourned Sine Die)***

Bill Title: Relating to images captured by unmanned aircraft and other images and recordings; providing penalties. [**Track Bill**]

Status: 2013-06-14 - Effective on 9/1/13 [HB912 Detail]

Download: Texas-2013-HB912-Enrolled.html

H.B. No. 912

AN ACT

relating to images captured by unmanned aircraft and other images and recordings; providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. This Act shall be known as the Texas Privacy Act.

SECTION 2. Subtitle B, Title 4, Government Code, is amended by adding Chapter 423 to read as follows:

CHAPTER 423. USE OF UNMANNED AIRCRAFT

Sec. 423.001. DEFINITION. In this chapter, "image" means any capturing of sound waves, thermal, infrared, ultraviolet, visible light, or other electromagnetic waves, odor, or other conditions existing on or about real property in this state or an individual located on that property.

Sec. 423.002. NONAPPLICABILITY. (a) It is lawful to capture an image using an unmanned aircraft in this state:

(1) for purposes of professional or scholarly research and development by a person acting on behalf of an institution of higher education, as defined by Section 61.003, Education Code, including a person who:

(A) is a professor, employee, or student of the institution; or

(B) is under contract with or otherwise acting under the direction or on behalf of the institution;

(2) in airspace designated as a test site or range authorized by the Federal Aviation Administration for the purpose of integrating unmanned aircraft systems into the national airspace;

(3) as part of an operation, exercise, or mission of any branch of the United States military;

(4) if the image is captured by a satellite for the purposes of mapping;

(5) if the image is captured by or for an electric or natural gas utility:

(A) for operations and maintenance of utility facilities for the purpose of maintaining utility system reliability and integrity;

(B) for inspecting utility facilities to determine repair, maintenance, or replacement needs during and after construction of such facilities;

(C) for assessing vegetation growth for the purpose of maintaining clearances on utility easements; and

(D) for utility facility routing and siting for the purpose of providing utility service;

(6) with the consent of the individual who owns or lawfully occupies the real property captured in the image;

(7) pursuant to a valid search or arrest warrant;

(8) if the image is captured by a law enforcement authority or a person who is under contract with or otherwise acting under the direction or on behalf of a law enforcement authority:

(A) in immediate pursuit of a person law enforcement officers have reasonable suspicion or probable cause to suspect has committed an offense, not including misdemeanors or offenses punishable by a fine only;

(B) for the purpose of documenting a crime scene where an offense, not including misdemeanors or offenses punishable by a fine only, has been committed;

(C) for the purpose of investigating the scene of:

(i) a human fatality;

(ii) a motor vehicle accident causing death or serious bodily injury to a person; or

(iii) any motor vehicle accident on a state highway or federal interstate or highway;

(D) in connection with the search for a missing person;

(E) for the purpose of conducting a high-risk tactical operation that poses a threat to human life; or

(F) of private property that is generally open to the public where the property owner consents to law enforcement public safety responsibilities;

(9) if the image is captured by state or local law enforcement authorities, or a person who is under contract with or otherwise acting under the direction or on behalf of state authorities, for the purpose of:

(A) surveying the scene of a catastrophe or other damage to determine whether a state of emergency should be declared;

(B) preserving public safety, protecting property, or surveying damage or contamination during a lawfully declared state of emergency; or

(C) conducting routine air quality sampling and

monitoring, as provided by state or local law;

(10) at the scene of a spill, or a suspected spill, of hazardous materials;

(11) for the purpose of fire suppression;

(12) for the purpose of rescuing a person whose life or well-being is in imminent danger;

(13) if the image is captured by a Texas licensed real estate broker in connection with the marketing, sale, or financing of real property, provided that no individual is identifiable in the image;

(14) of real property or a person on real property that is within 25 miles of the United States border;

(15) from a height no more than eight feet above ground level in a public place, if the image was captured without using any electronic, mechanical, or other means to amplify the image beyond normal human perception;

(16) of public real property or a person on that property;

(17) if the image is captured by the owner or operator of an oil, gas, water, or other pipeline for the purpose of inspecting, maintaining, or repairing pipelines or other related facilities, and is captured without the intent to conduct surveillance on an individual or real property located in this state;

(18) in connection with oil pipeline safety and rig protection; or

(19) in connection with port authority surveillance and security.

(b) This chapter does not apply to the manufacture, assembly, distribution, or sale of an unmanned aircraft.

Sec. 423.003. OFFENSE: ILLEGAL USE OF UNMANNED AIRCRAFT TO CAPTURE IMAGE. (a) A person commits an offense if the person uses an unmanned aircraft to capture an image of an individual or privately owned real property in this state with the intent to conduct surveillance on the individual or property captured in the image.

(b) An offense under this section is a Class C misdemeanor.

(c) It is a defense to prosecution under this section that the person destroyed the image:

(1) as soon as the person had knowledge that the image was captured in violation of this section; and

(2) without disclosing, displaying, or distributing the image to a third party.

(d) In this section, "intent" has the meaning assigned by Section 6.03, Penal Code.

Sec. 423.004. OFFENSE: POSSESSION, DISCLOSURE, DISPLAY, DISTRIBUTION, OR USE OF IMAGE. (a) A person commits an offense if the person:

(1) captures an image in violation of Section 423.003; and

(2) possesses, discloses, displays, distributes, or

otherwise uses that image.

(b) An offense under this section for the possession of an image is a Class C misdemeanor. An offense under this section for the disclosure, display, distribution, or other use of an image is a Class B misdemeanor.

(c) Each image a person possesses, discloses, displays, distributes, or otherwise uses in violation of this section is a separate offense.

(d) It is a defense to prosecution under this section for the possession of an image that the person destroyed the image as soon as the person had knowledge that the image was captured in violation of Section 423.003.

(e) It is a defense to prosecution under this section for the disclosure, display, distribution, or other use of an image that the person stopped disclosing, displaying, distributing, or otherwise using the image as soon as the person had knowledge that the image was captured in violation of Section 423.003.

Sec. 423.005. ILLEGALLY OR INCIDENTALLY CAPTURED IMAGES NOT SUBJECT TO DISCLOSURE. (a) Except as otherwise provided by Subsection (b), an image captured in violation of Section 423.003, or an image captured by an unmanned aircraft that was incidental to the lawful capturing of an image:

(1) may not be used as evidence in any criminal or juvenile proceeding, civil action, or administrative proceeding;

(2) is not subject to disclosure, inspection, or copying under Chapter 552; and

(3) is not subject to discovery, subpoena, or other means of legal compulsion for its release.

(b) An image described by Subsection (a) may be disclosed and used as evidence to prove a violation of this chapter and is subject to discovery, subpoena, or other means of legal compulsion for that purpose.

Sec. 423.006. CIVIL ACTION. (a) An owner or tenant of privately owned real property located in this state may bring against a person who, in violation of Section 423.003, captured an image of the property or the owner or tenant while on the property an action to:

(1) enjoin a violation or imminent violation of Section 423.003 or 423.004;

(2) recover a civil penalty of:

(A) $5,000 for all images captured in a single episode in violation of Section 423.003; or

(B) $10,000 for disclosure, display, distribution, or other use of any images captured in a single episode in violation of Section 423.004; or

(3) recover actual damages if the person who captured the image in violation of Section 423.003 discloses, displays, or distributes the image with malice.

(b) For purposes of recovering the civil penalty or actual damages under Subsection (a), all owners of a parcel of real

property are considered to be a single owner and all tenants of a parcel of real property are considered to be a single tenant.

(c) In this section, "malice" has the meaning assigned by Section 41.001, Civil Practice and Remedies Code.

(d) In addition to any civil penalties authorized under this section, the court shall award court costs and reasonable attorney's fees to the prevailing party.

(e) Venue for an action under this section is governed by Chapter 15, Civil Practice and Remedies Code.

(f) An action brought under this section must be commenced within two years from the date the image was:

(1) captured in violation of Section 423.003; or

(2) initially disclosed, displayed, distributed, or otherwise used in violation of Section 423.004.

Sec. 423.007. RULES FOR USE BY LAW ENFORCEMENT. The Department of Public Safety shall adopt rules and guidelines for use of an unmanned aircraft by a law enforcement authority in this state.

Sec. 423.008. REPORTING BY LAW ENFORCEMENT AGENCY. (a) Not earlier than January 1 and not later than January 15 of each odd-numbered year, each state law enforcement agency and each county or municipal law enforcement agency located in a county or municipality, as applicable, with a population greater than 150,000, that used or operated an unmanned aircraft during the preceding 24 months shall issue a written report to the governor, the lieutenant governor, and each member of the legislature and shall:

(1) retain the report for public viewing; and

(2) post the report on the law enforcement agency's publicly accessible website, if one exists.

(b) The report must include:

(1) the number of times an unmanned aircraft was used, organized by date, time, location, and the types of incidents and types of justification for the use;

(2) the number of criminal investigations aided by the use of an unmanned aircraft and a description of how the unmanned aircraft aided each investigation;

(3) the number of times an unmanned aircraft was used for a law enforcement operation other than a criminal investigation, the dates and locations of those operations, and a description of how the unmanned aircraft aided each operation;

(4) the type of information collected on an individual, residence, property, or area that was not the subject of a law enforcement operation and the frequency of the collection of this information; and

(5) the total cost of acquiring, maintaining, repairing, and operating or otherwise using each unmanned aircraft for the preceding 24 months.

SECTION 3. The change in law made by this Act applies only to the capture, possession, disclosure, display, distribution, or

other use of an image that occurs on or after the effective date of this Act.

SECTION 4. The provisions of this Act or the applications of those provisions are severable as provided by Section 311.032(c), Government Code.

SECTION 5. This Act takes effect September 1, 2013.

President of the Senate

Speaker of the House

I certify that H.B. No. 912 was passed by the House on May 10, 2013, by the following vote: Yeas 128, Nays 11, 2 present, not voting; that the House refused to concur in Senate amendments to H.B. No. 912 on May 21, 2013, and requested the appointment of a conference committee to consider the differences between the two houses; that the House adopted the conference committee report on H.B. No. 912 on May 26, 2013, by the following vote: Yeas 140, Nays 4, 2 present, not voting; and that the House adopted H.C.R. No. 217 authorizing certain corrections in H.B. No. 912 on May 27, 2013, by the following vote: Yeas 145, Nays 3, 2 present, not voting.

Chief Clerk of the House

I certify that H.B. No. 912 was passed by the Senate, with amendments, on May 17, 2013, by the following vote: Yeas 29, Nays 1; at the request of the House, the Senate appointed a conference committee to consider the differences between the two houses; that the Senate adopted the conference committee report on H.B. No. 912 on May 26, 2013, by the following vote: Yeas 26, Nays 5; and that the Senate adopted H.C.R. No. 217 authorizing certain corrections in H.B. No. 912 on May 27, 2013, by the following vote: Yeas 31, Nays 0.

Secretary of the Senate

APPROVED: _____

Date

_____

Governor

Privacy Impact Assessment
for the

Aircraft Systems

DHS/CBP/PIA-018

September 9, 2013

Contact Point
Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
(202) 344-3950

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) employs several types of aircraft including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or responses to other emergencies. Video, images, and sensor data collected through these Aircraft Systems alone cannot be used to identify a person, but they may later be associated with a person as part of a law enforcement investigation or encounter with CBP officers or agents. DHS/CBP is conducting this Privacy Impact Assessment to evaluate the privacy impact of these technologies on persons.

Introduction

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard. To achieve these missions, CBP employs several types of aircraft, including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or other emergencies. This Privacy Impact Assessment (PIA) is necessary because the aircraft are equipped with technology that captures information that may be associated with persons whom CBP encounters.

Overview

CBP employs several types of aircraft to achieve its mission objectives. All aircraft, manned or unmanned, have some type of imaging capability such as video, still images collection, and/or radar. The UAS differ from CBP's manned aircraft only in that the pilot controls the aircraft from the ground and the aircraft are capable of flying farther distances and longer hours continuously. All aircraft are owned and operated by the Office of Air and Marine (OAM); the Office of Intelligence and Investigative Liaison (OIIL) is responsible for processing, exploitation, and dissemination (PED) of imagery transmitted from aircraft.

CBP aircraft, both manned and unmanned, are used in the following scenarios: (1) to patrol the border; (2) to conduct surveillance for investigative operations; (3) to conduct damage assessment in disaster situations; and (4) in response to officer safety scenarios. While CBP also

allocates its air assets in a manner that reflects this prioritization, CBP reviews and considers all requests for assistance. Lastly, CBP does not equip its aircraft with weapons. While the crew in all manned aircraft and the officers and agents onboard the aircraft during tactical missions do carry weapons, the various aircraft are not equipped with armaments.

Helicopters

CBP operates several types of manned rotary-wing aircraft (helicopters) in support of its mission, notably, the American Eurocopter AS-350, Augusta Westland AW-139, Bell Huey UH-1, and Sikorsky UH-60. CBP uses helicopters for observation, for tracking suspects and supporting ground units, aerial reconnaissance of moving objects and persons, external lift capability for seizures and equipment delivery, and tactical support and transportation for law enforcement activities. Areas of operation include the border environment, both land and sea, to observe and interdict unlawful crossings of persons and goods, the airspace surrounding defined DHS National Special Security Events or critical venues, and populated or unpopulated areas that are the subject of defined law enforcement activity or investigation. CBP's helicopter fleet operates out of 30 locations maintained by OAM across the United States.

Fixed-wing Aircraft

CBP has manned fixed-wing P-3 AEW/LRT Orion aircraft operating out of specific operations centers in Corpus Christi, TX and Jacksonville, FL. CBP practices a defense in depth strategy of the borders of the United States and in active prosecution of attempts to smuggle persons or contraband by extending surveillance over international and coastal waters. As part of this strategy and as a means of integrating with the overall U.S. Government strategy to interdict the flow of narcotics and controlled substances across the U.S. southern borders, this defense in depth includes expanding the area of patrol to include the Caribbean and Eastern Pacific waters that border Source and Transit Zone countries.[1] Together the operations centers operate the P-3 aircraft primarily in Central and South America. Certain P-3s are used to intercept and track both aircraft and vessels for hours at a time while maintaining a covert standoff. CBP also operates several smaller, manned, fixed-wing aircraft out of OAM operational locations. These fixed-wing aircraft include piston-engine propeller-powered aircraft (Cessna models), larger turbo-prop powered aircraft (Bombardier Dash Eight, Pilatus, and Beechcraft Super King Air), and jet aircraft (Cessna Citation). These aircraft variously perform surveillance, tracking, interdiction, intercept, and information gathering roles. Fixed-Wing Aircraft employ various types of sensor technology including video, still, and radar images, and Law Enforcement Technical Collection (LETC) (electronic signals information across the electromagnetic spectrum).

[1] Source and Transit Zone countries are those nations working in partnership with the United States to interdict the flow of narcotics and controlled substances to the United States through the Caribbean Basin and along the coastal waters of the eastern Pacific Ocean. http://www.whitehouse.gov/ondcp/transit-zone-operations.

UAS

A UAS encompasses an unmanned aircraft, digital network, and personnel on the ground who operate the aircraft. CBP currently owns and operates ten such aircraft. The UAS aircraft include the Predator B[2] and the maritime variant of the Predator B, the Guardian, which allows CBP to conduct missions in areas that are remote, too rugged for ground access, or otherwise considered too high-risk for manned aircraft or personnel on the ground. The aircraft are stationed and principally controlled at four locations: Sierra Vista, AZ (4 aircraft); Grand Forks, ND (2 aircraft); Corpus Christi, TX (2 aircraft); and Cape Canaveral, FL (2 aircraft). CBP's UAS operate in accordance within the Federal Aviation Administration (FAA) Certificate of Authorization (COA) process. CBP works with the FAA to develop the COAs to define airspace for UAS operation. Consistent with the primary mission for the UAS, these COAs, which are in effect for a period of two years, define airspace (altitude, latitude, and longitude (geography)) along the border and outside of urban areas to support CBP UAS flight operations. As the FAA develops its roadmap to integrate UAS into the National Airspace System (NAS)[3], CBP will adjust to these new requirements and continue to employ UAS in pursuit of its primary border security mission.

Uses of Aircraft

Patrol

CBP uses all of its aircraft to patrol different parts of the border based on the specific strengths of the different aircraft. CBP P-3s patrol in a 42-million square mile area of the Western Caribbean and Eastern Pacific, known as the Source and Transit Zone, in search of drugs that are in transit towards U.S. shores. The P-3's distinctive detection capabilities allow highly-trained crews to identify emerging threats well beyond U.S. land borders. By providing surveillance of known air, land, and maritime smuggling routes in an area that is twice the size of the continental U.S., the P-3s detect, monitor, and disrupt smuggling activities before they reach shore.[4] As part of this patrol responsibility, images and radar information obtained in detecting, monitoring, or supporting activities is collected and maintained either for direct case support or to permit historical trend analysis regarding smuggling routes.

Along both the northern and southern borders CBP also employs UAS and smaller manned aircraft to help agents detect, identify, apprehend, and remove individuals and

[2] The General Atomics Aeronautical Systems MQ-9 Predator B is a mid-size Unmanned Aerial Vehicle (UAV) approximately thirty-six feet in length, with a maximum gross weight of 10,500 pounds and a wing span of sixty-six feet.

[3] See, *FAA Modernization and Reform Act of 2012*, Pub. L. No.112-95, sec. 331, 126 Stat. 11, 72, which mandates that the FAA prepare a roadmap to integrate UAS into the NAS by 2015.

[4] The Anti-Drug Abuse Act of 1988 established the Office of National Drug Control Policy (ONDCP) to set priorities, implement a national strategy, and certify Federal drug-control budgets. Interdiction of the flow of illicit drugs through the Source and Transit Zone is a critical component of the National Drug Control Strategy prepared annually by ONDCP.

contraband illegally entering the United States at and between Ports of Entry (POE). The COA defined airspace establishes operational corridors for UAS activity both along and within 100 miles of the border for the northern border, and along and within 25 to 60 miles of the border for the southern border, exclusive of urban areas. CBP helicopters and manned fixed-wing aircraft may operate in and around urban areas; however, the principal mission remains focused on those areas between the POE. Images, LETC, and radar information, specifically with respect to border areas between the POEs, are collected in support of case development or to permit trend analysis.

Following a flight, the images are provided to OIIL for processing, exploitation, and dissemination. Subsequently, and only upon request, OIIL provides access to the forensic analysis of a particular image and area to authorized persons who have a "need to know;" when the dissemination is in response to a particular law enforcement activity or case, that analysis may include PII.

Persons who are apprehended and who were video recorded from a UAS or a manned aircraft may have the video of their crossing and/or apprehension associated with a case file that contains their PII.

Separately, CBP also deploys manned fixed-wing aircraft with LETC sensors over the border area in support of its counter-terrorism and interdiction of smuggling operations. The LETC sensors permit surveillance of the electromagnetic spectrum for the purpose of identifying organized border crossing activity between the ports of entry.

Investigative Operations

CBP uses both UAS and manned aircraft in support of other DHS components, such as U.S. Immigration and Enforcement (ICE), or other federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI) or Drug Enforcement Agency (DEA). Requests for aircraft support that are related to the border surveillance must be directed to the Assistant Commissioner, OIIL, for authorization. Each request for information follows a standard process and is reviewed and considered in terms of the requesting agencies' authorities to receive the sought after information, CBP's own authority to lend assistance, and CBP's ability to integrate the information collection into its mission. Separately, OAM must determine the availability of aircraft type and the integration of the requested activity into its flight operations.

Typical support missions include overhead observation of previously identified persons, specified locations, and particular conveyances for enhanced situational awareness and increased officer safety. For example, the UAS could conduct surveillance over a building to inform ground units of the general external layout of the building or provide the location of vehicles or individuals outside the building. When flying a UAS in support of another component or government agency for an investigative operation, CBP may provide the other agency with a direct video feed through access controls or with a downloaded video recording of the operation,

in whole or in part, based on the request. Similarly, CBP may deploy a helicopter or manned fixed-wing aircraft to provide over top visibility into a developing incident. Video images from the Electrical Optical/Infrared ball (EO/IR) ball are fed through the DHS firewall to "Big Pipe," a video and image distribution network operating within the CBP/DHS firewall, to identified users, analysts, and decision makers for real-time mission support and border protection.

Disasters

The P-3 may be used to conduct reconnaissance missions during natural disasters in support of FEMA. During these missions, P-3s can provide near real-time, high quality video of affected areas to first responders and FEMA. P-3s are equipped with similarly capable EO/IR Ball cameras; the images are also fed through a transmission to a ground station where the video is decrypted and fed to Big Pipe to disseminate inside the DHS firewall to authorized users within DHS and any other requesting agency.

UAS may also be used outside existing COAs during natural disasters once the government has issued a disaster declaration. For example, the UAS may fly missions in support of other government agencies such as the National Oceanic and Atmospheric Administration (NOAA) or FEMA to provide video or radar images of flooding. In disaster situations, CBP works with the FAA to construct a COA defining the airspace where a CBP UAS may operate. The UAS may provide a real-time feed during flight through Big Pipe or, subsequently, an analyzed image comparing the raw feed to an image with identified details, noting changes, to FEMA, state emergency operations centers, United States Geological Survey (USGS), and/or the Army Corps of Engineers. Video from these operations are not used to identify individuals. As with other requests for support, disaster area overflight requests are assigned in accordance with the national policy regarding the tasking of CBP air assets.

Officer Safety and Support to State and Local Law Enforcement

State and local law enforcement officials may request aircraft support (e.g., UH-60, P-3, UAS) in emergency situations; often this involves circumstances when officer safety is implicated, and in which aerial surveillance is necessary or the terrain would be too difficult for law enforcement personnel to navigate. OIIL reviews each request to determine whether to respond and OAM reviews how and in what context it may respond. Based on both organizations within CBP, a decision is made whether to provide assistance. Access to video taken during emergency situations may be provided, either at a DHS/CBP facility or by temporarily granting direct access through the DHS firewall. Sharing of this information with state, local, or other government agencies is on a case by case basis as determined through CBP's Request for Information process.

As in the mission uses discussed above, UAS and manned aircraft offer several options for deploying information gathering equipment. The UAS can serve as force multiplier insofar as the UAS enables the monitoring of large areas of land more efficiently and with fewer

personnel than other aviation assets. UAS can enhance situational awareness and increase officer safety by providing aerial support to officers on the ground by monitoring a fixed location while flying at a high altitude to reduce the likelihood of detection. Manned aircraft offer the ability to fly in more congested airspace and to transport officers, agents, equipment, and seized assets.

Technology on Board the Aircraft

The various aircraft have different types of surveillance technology. Most aircraft, manned and unmanned have an EO/IR ball attached to provide a means of collecting information. The EO/IR ball installed on the UAS also assists the pilot during take-off and landing. While the cameras on each aircraft are not identical, they have almost identical performance specifications. The EO/IR ball is a camera, which employs a fixed-focus lens, that is capable of providing video at any altitude and allows operators, using digital zooming (software based image enhancement), to take small-scale aerial video images of buildings, vehicles, and people. Aircraft altitude directly affects a fixed-focus camera's performance; the higher the aircraft's altitude, the less detail an operator is able to see.

A lower altitude permits the EO/IR ball to provide greater detail in an image, which may permit identification; this observation activity, however, does not occur unnoticed or subject to attempts at evasion, and therefore is more often part of a defined law enforcement operation. Persons are often successful at hiding their identity from known surveillance aircraft by simply looking away.

At present, the flight and mission parameters for the UAS place their operation within an altitude block of 19,000 to 28,000 feet, thereby effectively limiting the altitude for the EO/IR ball on a UAS to a minimum of 19,000 feet. At this minimum altitude, the camera does not provide enough detail for an operator to identify a person (that is to discern physical characteristics such as height, weight, eye color, hair style, or a facial image). The camera operator may have enough detail to identify whether an individual is carrying a long gun or wearing a back pack. At an altitude of 19,000 feet the camera operator cannot read a license plate, nor are license plate readers effective.

Conversely, the flight parameters for helicopters and fixed-wing aircraft are broader in terms of altitude and geography; their flight operations are integrated into the NAS and do not require a COA. The mission parameters and physical capabilities for helicopters and manned fixed-wing aircraft, however, place different operational restrictions upon the aircraft.

The EO/IR ball can provide daytime or nighttime visual video observation of movement or objects on the ground. The images, depending upon the aircraft deploying the camera, tend to be small in scale, to provide environmental context. A principal purpose for tracking a person or vehicle from an aircraft with an EO/IR ball is to assist CBP or law enforcement personnel on the ground with information to permit a safe encounter—this requires environmental context more

than a best possible close-up of a face. When viewing vehicles, an operator can distinguish a car from a truck, and depending on the altitude at which the aircraft is flying, may be able to identify the model of the vehicle. During daytime flights, an operator may also be able to determine the color of the vehicle. The images of vehicles and/or individuals recorded by the EO/IR ball are not associated with any biographical information unless the individual is apprehended, at which point the video may be associated with the Personally Identifiable Information (PII) contained within the individual's case file.

In addition to EO/IR CBP deploys a UAS stationed along the Southwestern border in Sierra Vista, AZ, with the Wide Area Surveillance System (WASS). WASS uses a sensor mounted to the wing of a UAS to sweep large areas of border territory (approximately six kilometers in width) as the aircraft moves along its flight path. WASS alerts CBP to the existence of persons and/or vehicles along the border and provides coordinates to determine their location. The UAS pilot and sensor operator can then inform ground units of the location so that Border Patrol may coordinate an interdiction of the persons or vehicles. WASS provides a radar sensor image, which CBP may share through Big Pipe during operation.

Some manned and unmanned aircraft are also equipped with synthetic aperture radar that can provide black and white images in all weather. This radar can provide silhouettes of people and vehicles, but provides no identifying details. Using this technology, an operator is not able to pick up identifying characteristics of a person or a vehicle. The synthetic aperture radar is primarily used for change detection. For example, the operator can identify tire tracks on the ground that were not present in prior images provided by the radar. Similarly, an operator can use the synthetic aperture radar to determine the extent of flooding in a particular region by noting the changes to the topography.

Certain manned fixed-wing aircraft deploy LETC sensors used to detect electronic signals in the electromagnetic spectrum. These specifically designed aircraft operate in support of counter-terrorism efforts and to interdict organized smuggling (people, contraband, and controlled substances) operations within the border area. Like with the EO/IR ball, information from LETC sensors may be employed to support officers and agents on the ground as they move to a position where they can safely encounter observed persons. LETC aircraft sensors are solely deployed on manned fixed-wing aircraft.

Data on the digital video recorders on CBP aircraft are maintained for a maximum of 30 days and then overwritten by new data. The images and related data from CBP aircraft, both manned and unmanned, are provided through Big Pipe to identified users, analysts, and decision makers for real-time mission support and border protection. Images from the EO/IR ball mounted on the UAS are sent by an encrypted transmission, first to the satellite providing the control signals, and then, again by encrypted transmission, to the ground control station where the pilot and sensor operator are located. The image data is decrypted and brought inside the

DHS firewall at the ground control station, where Big Pipe can ingest the data and provide a feed to assigned users and analysts.

Big Pipe is a fully distributed network hosted by CBP and supports not only event-based law enforcement missions, but also FEMA's National Response Framework.[5] Big Pipe employs role-based access controls to provide users possessing a need to know access to distinct video feeds at command centers, other CBP/DHS locations, and for authorized persons with technical access through the DHS firewall. OAM retains control over defining users for Big Pipe and assigning access. After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data. Stored data is retrieved based on the date and time of the mission and only by authorized users on a need to know basis. If data is used for investigative purposes, and associated with a particular individual it goes into a case management system, which is covered by the corresponding Privacy Act System of Records Notice (SORN) for the case management system. Big Pipe, separately, provides a feed of video and radar images from UAS to the Air and Marine Operations Center (AMOC), where OIIL operates one of several PED cells to review this data over time to perform trend analysis and change detection. Video and radar images maintained by a PED cell, such as at the AMOC, are stored on a separate server dedicated to the PED cell mission for up to five years. The analyzed images may be shared by OIIL in response to law enforcement needs.

Summary of Privacy Risks

The use of these aircraft and accompanying surveillance technologies presents several privacy concerns. The first concern is ensuring that CBP's collection and use of data from aerial surveillance remains within the scope of its authorities to protect the border and provide support for law enforcement activities, while continuing to preserve a person's right to privacy. CBP's border security mission has a broad mandate to determine the admissibility of persons and ensure that goods are not introduced into the United States contrary to law.[6] Similarly, the statutory language in CBP's annual appropriations directs CBP Air and Marine to provide integrated and coordinated border interdiction and law enforcement support for homeland security missions, including assistance to federal, state, and local agencies and emergency humanitarian efforts; to provide airspace security for high-risk areas or National Special Security Events[7]; and to combat

---

[5] The National Response Framework is a DHS/FEMA led effort, which provides the guiding principles that establish a comprehensive, national, all-hazards approach to domestic incident response—from the smallest incident to the largest catastrophe. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

[6] Title 8, United States Code (U.S.C.), sections 1225, 1357, other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations.

[7] See Title 18 U.S.C. Section 3056, which authorizes the designation of National Special Security Events.

efforts to smuggle narcotics and other contraband into the United States[8]. Deploying OAM's various air assets to support these missions improves DHS/CBP's capability to obtain streaming video, and to assess critical infrastructure before and after events.

CBP's use of manned and unmanned aircraft to conduct aerial observations is consistent with CBP's authorities and obligations. To the extent that aircraft flying in support of tactical operations overfly private residences, there is a minimal risk that a person's privacy might be unintentionally violated. The images captured are not personally identifiable without further investigative information. Neither manned nor unmanned aircraft physically intrude upon or disturb the use of private property. Further, the cameras deployed on UAS or manned aircraft do not have the capability to see through walls or otherwise collect information regarding what occurs in the interior of a building, nor is that their purpose. UAS operate primarily at an altitude between 19,000 and 28,000 feet pursuant to their COA approved by the FAA, and are focused as previously described.

A second privacy concern, specific to UAS, is that they present a perceived risk to privacy because they are able to fly for longer hours than manned aircraft and conduct surveillance undetected. Like other aircraft, UAS are useful for monitoring remote land border areas where patrols cannot easily travel and infrastructure is difficult or impossible to build. Unlike manned aircraft, UAS are operated by personnel on the ground, allowing the crew to be relieved while the UAS is still in the air. This capability allows UAS to provide long-range surveillance for greater lengths of time than manned aircraft. Because of their small size compared to manned aircraft, and the altitude at which UAS can operate, these physical attributes may serve to conceal the presence of a UAS and reduce detection of their operating noise while still being able to maneuver over a small area and provide surveillance. Other OAM operated long range fixed-wing aircraft cannot steadily monitor a set location because of their size and turning radius. Helicopters are more easily detected because of their noise and lower operational altitudes. This means that, unlike fixed-wing aircraft and helicopters, UAS can monitor either a moving target or a fixed location for relatively longer periods of time without the likelihood of detection.

While UAS can fly for longer periods of time, they are equipped with the same technology to conduct surveillance that is presently deployed on CBP manned aircraft. The only sensor available on UAS that is not used by CBP manned aircraft currently is the WASS sensor. The WASS sensor can only detect the presence of a person and track his or her movements (much the same way other radar technology can detect an object and track its movement); it cannot be used to identify a person. The WASS sensor is designed to sweep large areas of land and is only used to patrol along the southwest border and to assist with interdictions. Other technologies on the UAS are shared by CBP's manned aircraft. Putting these technologies on a

[8] See National Drug Control Strategy, http://www.whitehouse.gov/ondcp/2013-national-drug-control-strategy.

UAS only enhances CBP's ability to perform its existing functions. For instance, CBP's surveillance video of a location used to smuggle persons or contraband using a UAS instead of a P-3 may be longer in duration with less interruption and less likelihood of detection.

To mitigate the risk presented by longer sustained surveillance of an individual or residence without the individual's knowledge, CBP has strict mission priorities for UAS and all aircraft operations. For instance, CBP aircraft may only be used in support of an authorized mission or investigation, the video or other data collected from CBP aircraft may only be accessed by authorized personnel with an authorized need to know, and the CBP-held video or other data is controlled through chains of custody and stored in secure locations until it is destroyed. In addition, the FAA requires CBP to construct a COA, in the instance of deploying a UAS, for a duration determined by the investigative activity or emergency circumstance, before conducting an operation away from the border and already established COAs.

The third privacy concern, unique to UAS, pertains to the security of the system itself and the potential for hijacking of the unmanned aircraft. CBP has taken several steps to protect UAS against potential hackers. All UAS are controlled and monitored at all times by operators in ground control stations using satellite communication that is relayed through an encrypted data feed. The ability to interfere with such an encrypted data feed requires disrupting the signal from satellite to UAS, for the purpose of acquiring the data feed or controlling the UAS. In the event that the ground control station loses its ability to control the UAS, another ground control station can pick up control of that UAS. The UAS use redundant navigation systems and GPS receivers so that if a signal is lost or someone attempts to override the signal, the UAS relies on these other systems and the GPS receivers for flight operations. In order to protect the airspace, the FAA is notified immediately if a UAS loses its signal. Furthermore, if communication between ground control and the UAS is ever interrupted or lost, the UAS are pre-programmed to fly to a pre-coordinated point in a remote location to orbit while waiting for the signal to be reestablished, or to continue to orbit this Flight Termination Point until the aircraft runs out of fuel and crashes.

Because of the unique privacy concerns raised by CBP's use of Aircraft Systems, CBP has conducted this PIA to evaluate the privacy risks associated with the use of Aircraft Systems and to enhance public understanding of the authorities, policies, procedures, and privacy controls related to that use.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[9] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. Given that Aircraft Systems and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records pertaining to an individual that would be subject to the parameters of the Privacy Act, this PIA is conducted to relate the use of these observation and data collection platforms to the DHS construct of the FIPPs. This PIA examines the privacy impact of Aircraft Systems operations as it relates to the DHS FIPPs.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

This PIA provides a level of transparency to the public about the current surveillance programs undertaken by CBP. The video, still images, signals information, and/or radar images do not clearly identify individuals. The only information about individuals that is collected and/or retained is the indication of a human form. These images, however, may be associated with a person if the person is apprehended. For example, video collected by an EO/IR ball may show several individuals traversing the land border and being intercepted by officers or agents of CBP. While the video resolution or radar mapping images are not sufficiently precise to permit actual identification, the circumstances of CBP interdiction and apprehension of a suspect in conjunction with the aerial surveillance are sufficient to link the indistinct images of persons traversing the ground to the case file. Individuals who are apprehended by CBP as a result of observation by aircraft at or near the border may have video of their crossing and apprehension associated with their enforcement case file. CBP obtains biographical data pertaining to the apprehended person at the moment of apprehension. CBP stores all biographical information

[9] DHS Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008.

obtained from apprehended individuals and any video or radar images of their movement obtained from the aircraft in the appropriate law enforcement case management system.

When CBP associates video, still images, signals information, and/or radar images with an individual after apprehension, that information becomes subject to the requirements of the Privacy Act in the same manner and to the same extent that the apprehension of the individual becomes a record in a Privacy Act system. The Privacy Act requires that agencies publish a SORN in the Federal Register describing the nature, purpose, maintenance, use, and sharing of the information. This PIA serves as notice to the public that information captured by Aircraft Systems may become subject to the Privacy Act once it is associated with an individual.[10] Additionally, the video images associated with an individual's case file are covered by the appropriate law enforcement case management SORN, which maintains the case file. CBP will periodically re-assess the means by which the images from the aircraft are retrieved to determine whether the requirement for a SORN is triggered.

2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

Individual participation provides complementary benefits for the public and the government. The government is able to maintain the most accurate information about the public, and the public is given greater access to the amount and uses of the information maintained by the government. A traditional approach to individual participation is not always practical or possible for CBP, which has law enforcement and national security missions. Aircraft are primarily used to sweep the border area to locate individuals who are crossing the border illegally. Allowing an individual to consent to the collection, use, dissemination, and maintenance of video, still images, and/or radar images would compromise operations and would interfere with the U.S. government's ability to protect its borders, thereby lessening overall homeland security.

Individuals do not have the opportunity to restrict CBP's ability to collect information in the public sphere. Any information associated with an individual is part of a case file that is created as part of a law enforcement investigation or encounter.[11] Providing individuals of interest access to information about them in the context of a pending law enforcement

[10] For example, video information from an aircraft of an apprehension of a person at the border that is identified to that person would be referenced in the case notes pertaining to that person's apprehension in TECS (DHS/CBP – 011 TECS System of Records Notice December 19, 2008 73 FR 77778)

[11] CBP also incorporates images from surveillance or encounters into reports and analyses maintained in the Analytical Framework for Intelligence (AFI) (DHS/CBP – 017 System of Records June 7, 2012 77 FR 13813).

investigation may alert them to or otherwise compromise the investigation. Consequently, there is no mechanism for correction or redress for the video collected by the aircraft. Once that video is associated with an individual's case file, the individual must follow the procedure outlined in the corresponding privacy documents for that system. While individuals cannot participate in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them. More information on redress is provided below.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

The purpose specification principle requires DHS to 1) articulate the authority to retain the PII in question; and 2) articulate the purpose(s) for which DHS uses the PII.

CBP is authorized to collect video, other images, signals information, and data using aircraft in support of its border security mission and pursuant to the appropriations language mandating support for law enforcement as part of the mission of CBP Air and Marine.[12] Together, these authorities allow CBP to obtain information in support of border interdiction of narcotics and other contraband, the prevention of the illegal entry of aliens into the United States, the security of airspace for high-risk areas or National Special Security Events, and in support of federal, state, and local law enforcement, counterterrorism, and emergency humanitarian efforts.

CBP may use video, still images, signals information, and/or radar images, obtained from aircraft, to apprehend individuals and to provide evidence of an illegal border crossing or other violation of law. Consistent with applicable laws and SORNs, the information may be shared with other state, local, federal, tribal, and foreign law enforcement agencies in furtherance of enforcement of their laws.[13]

Video, still images, and/or radar images collected during investigative operations as part of a law enforcement investigation are used for enhanced situational awareness and increased officer safety, and may be used to provide evidence of a violation of law. These images are maintained in association with the investigative or case file that they support; their retention is managed by the same SORN and follows the handling of the investigative or case file.

---

[12] *See, e.g.*, H.R. REP. No. 112-91, at 46 (2011) stating "CBP Air and marine provides integrated and coordinated border interdiction and law enforcement support for homeland security missions; provides airspace security for high risk areas or National Special Security Events upon request; and combats efforts to smuggle narcotics and other contraband into the United States. CBP Air and Marine also support counterterrorism efforts of many other law enforcement agencies."

[13] *See* Consolidated Appropriations Act of 2012, Pub. L. No. 112-74 (2011), providing for "the interdiction of narcotics and other goods; the provision of support to Federal, State, and local agencies in the enforcement or administration of laws enforced by the Department of Homeland Security; and at the discretion of the Secretary of Homeland Security, the provision of assistance to Federal, State, and local agencies in other law enforcement and emergency humanitarian efforts…."

Video, still images, and/or images collected in natural disaster and/or emergency situations are used for relief work and disaster reconnaissance. CBP typically provides a direct feed of the video captured by aircraft in these scenarios to provide support to FEMA or state emergency operating centers. Video, still images, and/or radar images are not associated with an individual and are only used to indicate where an individual or group of individuals may be for emergency response purposes.

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

CBP seeks to minimize the collection and retention of video, signals information, and radar to that which is necessary and relevant to carry out CBP's mission. Accordingly, when aircraft are flown to patrol the border, they are authorized to fly the designated border surveillance mission area to ensure they are only capturing images and information necessary to detect, identify, apprehend, and remove persons and their possessions illegally entering the United States at and between POE. When aircraft are flown for investigative operations, officer safety incidents, or natural disaster reconnaissance, CBP approves and defines the specific mission that is authorized, and in the case of UAS, works with the FAA to construct a COA to establish airspace for that specific UAS operation. The video (that has not been associated with a case) remains on the digital video recorder originally used for recording until it over-written through re-use, which is after approximately 30 days.

After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data.

The information collected by the aircraft is not subject to the Privacy Act unless it is retrieved by using an individual's name or other unique identifier. If an individual is apprehended by CBP as a result of observation by aircraft or subsequent association from the presence of CBP assets, CBP may have video of that individual's apprehension associated with his or her enforcement case file. That video is retained according to the retention schedule of the SORN of the corresponding case management system. Video and Radar images obtained from UAS patrols of the border are also provided to PED cells operated by OIIL for use in analyses and intelligence products concerning historical, change detection (e.g., natural and man-made alterations to geography) along the border, and patterns of movement of persons across the border. This unassociated data, in conjunction with meta-data (such as latitude, longitude, date and time of the imagery) is retained for a maximum of five years.

5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

CBP only collects video and/or radar images, and signals information via aircraft pursuant to its law enforcement authority, as part of its border security mission, or when flying a mission in support of another agency, and when that other agency's authority covers the mission either through delegation of authority or direct control of the information collected. For example, CBP has provided support to the U.S. Forest Service in response to large scale wild fires to permit an overview of the extent and scale of the fire and identification of hot spots; this activity is pursuant to a request from the Forest Service, is performed pursuant to their authority, and the images are conveyed through designated access to the Big Pipe video distribution service. While the video resolution, radar mapping images, and signals information are not sufficiently precise to permit actual identification of a person, the images or information may be associated with an individual from context within the image, circumstances surrounding the activity occurring in the image, or additional information obtained directly from the person by an officer or agent. The images or information are only associated with an individual if the individual is apprehended or if the images are taken as part of an ongoing law enforcement investigation. Accordingly the data can only be used for the purposes specified in section 3 of this PIA.

CBP has procedures and processes in place for sharing any data collected by aircraft, including when that information becomes associated with a case and is used as evidence against an apprehended individual. In addition, all requests for aerial surveillance for intelligence gathering purposes must receive prior approval by the Assistant Commissioner, OIIL, before the air asset can conduct the flight. Similarly, requests for analytical products incorporating historical analysis of the border topography must be approved by the Assistant Commissioner, OIIL.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

As explained in section 4 (above), to ensure that the PII captured by aircraft is relevant and timely, any video, still images, signals information, and/or radar images must be associated within 30 days with the individual CBP apprehends, or the video/digital image is overwritten by OAM. Video and/or radar images are of no continuing value in a law enforcement support context unless they are associated with an individual during an apprehension because the video resolution or radar mapping images are not sufficiently precise to permit actual identification of

individuals. Video and/or radar images that are not associated with a person provide value in an intelligence context for helping to demonstrate the state of change occurring over time along the border. These unassociated images are separately maintained by OIIL for a maximum of five years.

To preserve the quality and integrity of the information collected that is used as evidence, CBP requires its officer/agents to successfully complete training on the proper operation of the recording equipment on its aircraft. The training includes correct techniques to copy recorded evidence from a non-portable hard drive to portable digital media and procedures to ensure that such evidence is not co-mingled with data from other investigations. The training also includes procedures to maintain an adequate chain of custody for all recorded evidence. Each officer/agent making a recording must ensure that the time and date shown in the original recording is accurate. After a mission is completed, the officer/agent must ensure that the original record is transferred entirely, in its original format, to portable media. The transferred data must not be edited or altered in any way. The officer/agent making the recording must label all copies of portable media with the corresponding case number (if available), the date and place of the original recording, and the names of the officer/agent and aircraft commander. The officer/agent making the recording must also label, initial, and maintain possession of the evidence until custody is properly transferred to the appropriate designated evidence custodian, case agent, Assistant United States Attorney, or other appropriate government official. As with any information associated with a case file, once the images are cross referenced to an investigation or case, they become covered by the system of records for that case file system and subject to the access and amendment provision of that system.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

CBP has taken steps to protect live video feeds, signals information, and recorded video, radar, and/or still pictures captured by its aircraft. Live video and flight information, which are sent from the UAS, are passed along an encrypted feed from the UAS through the satellite relay to the ground control station. Similarly, control information from the ground control station to the UAS also passes along an encrypted feed. Video and data transmitted in real time via Big Pipe, a closed system with restricted access, is subject to access controls and an approval process requiring clearance by one of two CBP/OAM system administrators to ensure that only authorized users with a need to know have access to the video feeds. The real time video feeds are not recorded and archived. Any recorded images that are saved to be used as evidence or for intelligence gathering must be handled in accordance with CBP policy. Images that are used as evidence must be handled according to the procedures detailed in section 6 of this PIA. All

recorded evidence must be kept in a locked container, segregated from other property and/or equipment. Video that is collected during an investigative operation that contains sensitive analytical surveillance, or reconnaissance related data may not be disclosed unless a request for disclosure has been submitted to the OIIL Collections Division Director. The request must include a copy of the information that is to be disclosed, must clearly specify the name of the intended recipient, how the information will be used, and the reasons justifying the disclosure. In the event that the information is disclosed, the OIIL Collections Division Director or his/her designee is required to redact law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a need-to-know.

8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

All CBP employees are required to complete annual privacy awareness training, in addition to training on ethics and the CBP Code of Conduct. Access controls, both physical and technological, are in place to ensure only authorized access to the aircraft systems and the collected data/images.

Moreover, CBP requires its employees to successfully complete training on techniques to copy recorded evidence to portable digital media and requires them to follow procedures to ensure that such evidence is not co-mingled with data from other investigations. Employees must follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

OIIL has a process in place for restricting the dissemination of video, still images, and radar images and keeps a log of the disclosures. Also, OIIL redacts law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a valid need-to-know. Separately, CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.

Conclusion

CBP operates aircraft systems in support of its border protection and law enforcement support missions. These systems provide a variety of mobile platforms from which to obtain signals information, video, still, and radar images of persons and vehicles in the border area or that are the subject of an investigation or law enforcement activity. The collection of these images and signals information complies with the same internal procedures and practices required of any surveillance using any means by CBP officers and agents. The distinct capabilities of the different aircraft operated by OAM enhance CBP's ability to conduct certain missions pertaining to information collection, surveillance, or reconnaissance; however, the processes and procedures for authorizing and accounting for how, when, and where information is obtained remain consistent with CBP's traditional border security and law enforcement practices and policy. As technology improves, operating environments change, and policies adapt, this PIA will be updated and amended to refresh the analysis of these changes on the privacy of persons, who directly or indirectly come into contact with the information and data collection activities associated with CBP Air operations.

Responsible Officials

Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
202-344-3950

Laurence Castelli
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
202-325-0280

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security