Community Policing & Unmanned Aircraft Systems (UAS)

Guidelines to Enhance Community Trust

Maria Valdovinos
James Specht
Jennifer Zeunik

COPS
Community Oriented Policing Services
U.S. Department of Justice

POLICE FOUNDATION

This project was supported by cooperative agreement number 2013-CK-WX-K002 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, companies, products, or services should not be considered an endorsement by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

This document contains preliminary analysis that is subject to further review and modification. It may not be quoted or cited and should not be disseminated further without the express permission of the Police Foundation or the U.S. Department of Justice. Any copyright in this work is subject to the Government's Unlimited Rights license as defined in FAR 52-227.14. The reproduction of this work for commercial purposes is strictly prohibited. Nongovernmental users may copy and distribute this document in any medium, either commercial or noncommercial, provided that this copyright notice is reproduced in all copies. Nongovernmental users may not use technical measures to obstruct or control the reading or further copying of the copies they make or distribute. Nongovernmental users may not accept compensation of any manner in exchange for copies. All other rights reserved.

The Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the author(s) nor the COPS Office can vouch for their current validity.

Recommended citation:
Valdovinos, Maria, Specht, James, and Zeunik, Jennifer 2016. *Community Policing & Unmanned Aircraft Systems (UAS): Guidelines to Enhance Community Trust*. Washington, DC: Office of Community Oriented Policing Services.

Published 2016

Contents

Letter from the Director . . . . . **vii**
Acknowledgements . . . . . **viii**
Executive Summary **1**
I – Background **3**
Police Foundation/COPS Office Community Policing and UAS Project 3
Chapter 1 . . . . . **5**
Community Policing and UAS **5**
Summary 6
Chapter 2 . . . . . **7**
UAS Terms and Technology **7**
UAS technology 7
sUAS features 7
Choosing a sUAS 8
Evolving technology 9
Usage of the terms drone, UAS, and sUAS 10
Summary 11
Chapter 3 . . . . . **12**
Evolution of UAS **12**
Military use of UAS 12
Commercial use of UAS 12
Summary 13
Chapter 4 . . . . . **14**
UAS Cost-Benefit Research **14**
Cost-benefit research 14
Comparing manned and unmanned aircraft units 14
Comparing costs based on mission 15
Tools for conducting UAS cost-benefit research 15
Cultivating funding for UAS acquisition 15
Summary 16
Chapter 5 . . . . . **17**
UAS and Law Enforcement **17**
Police-community partnerships 17
Benefits of UAS 17

Challenges in implementation . . . 19
Responding to increased use of UAS in the community . . . 19
Summary . . . 21
II – Legal and Regulatory Analysis. . . . 22
Chapter 6 Constitutional Law . . . 23
Summary . . . 25
Chapter 7 State Legislation . . . 26
Summary . . . 27
Chapter 8 Federal Aviation Administration Regulations . . . 28
Summary . . . 29
Chapter 9 Community Concerns & Liability . . . 30
Accountability: a key component of community policing . . . 32
Summary . . . 32
III – Determining Whether Your Community is Ready for UAS Technology: Conducting a Needs Assessment . . . 33
Chapter 10 Building Dialogue with the Community and Stakeholders . . . 34
The community's role in the sUAS program . . . 34
Final determination of need . . . 37
Summary . . . 37
Chapter 11 Developing an Operating Plan . . . 38
Components of the plan . . . 38
Recommended standards for UAS operations. . . . 39
Summary . . . 39
IV – sUAS Program Planning. . . . 40
Chapter 12 Developing Departmental UAS Policy, Procedures, and Guidelines . . . 41
Checklist for developing UAS policy and procedures . . . 41
Prohibitions . . . 42
U.S. Department of Justice guidelines for Federal law enforcement use of UAS . . . 43
Summary . . . 43
Chapter 13 Staffing and Training the sUAS Team. . . . 44
Staffing . . . 44
Chain of command . . . 45
Training . . . 45
Summary . . . 45
Chapter 14 Leveraging the Media to Communicate with the Community . . . 46
Traditional media & UAS . . . 47
Social media & UAS . . . 47
Summary . . . 48

V – Program Implementation **49**
Chapter 15 Program Implementation and Evaluation. **50**
Program implementation 50
Community engagement during implementation. 50
UAS operations 51
Program evaluation 51
Summary 52
Chapter 16 Ongoing Community Engagement **53**
Summary 54
VI – Conclusion. **55**
Notes on Research Methods **56**
Appendix 1 UAS Cost-Effectiveness Issues **57**
Appendix 2 Summary of UAS Legislation **58**
Appendix 3 Checklist for Planning and Implementation of a Law Enforcement sUAS Program. **63**
Conduct background research 63
Conduct a needs assessment 63
Planning and preparation 63
Implementation and maintenance 64
Appendix 4 Sample Press Release **65**
Appendix 5 Mesa County (Colorado) Sheriff's Office UAS FAQs **66**
Appendix 6 Arlington (Texas) Police Department UAS FAQs. **70**
Appendix 7 Arlington Police Department UAS Use Report. **72**
Appendix 8 International Association of Chiefs of Police (IACP) 2012 UAS Guidelines. **77**
Appendix 9 Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations. **80**
Appendix 10 Sample Privacy Impact Assessment **92**
Appendix 11 UAS Legal Memoranda **112**
Overview of UAS/UAV Technology and Regulation; Analysis of Police Use of UAS/UAV Systems Under U.S. Constitution and Case Law 112
Legal Analysis of UAV-Collected Data: Notice, Retention, Use. 151
Police Use of UAVs: Liability Analysis and Risk Management Considerations 174
Overview of UAS/UAV-Related State Legislation. 186
Building Public Understanding, Acceptance, and Confidence in Responsible and Constitutional Use of UAS Technology by Law Enforcement 211
UAS/UAV Related Publications, Law Review Articles, Research, and Peer Review Sources . . . 217
Appendix 12 Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure **232**
Appendix 13 Arlington (Texas) Police Department UAS Standard Operating Procedure **247**

Appendix 14 Department of Justice Policy Guidance 261
Appendix 15 International Association of Chiefs of Police (IACP) sUAS Concepts and Issues Paper and Model Policy. 266
Appendix 16 International Association of Chiefs of Police (IACP) Technology Policy Framework. 273
Glossary 284
References 285
About the Police Foundation 292
About the COPS Office 292

Letter from the Director

Dear Colleagues,

Implementing a significant advancement in law enforcement technology – unmanned aircraft systems (UAS) – is not a simple process. Though these systems, commonly known as drones, offer immeasurable tactical benefits, they also require a great deal of preparation, training, and community involvement in the guidelines for their use. As the authors point out, UAS could one day become the "Airborne Partners" of every public safety officer. But this cannot happen unless the public trusts that these airborne technologies are also their partners, working for the benefit of all.

To help law enforcement departments decide whether to adopt this technology and assist them in successfully implementing it if they do, the Police Foundation has developed this handbook, *Community Policing & Unmanned Aircraft Systems: Guidelines to Enhance Community Trust*, as a comprehensive guide to all aspects of drone use for law enforcement, including not only operational, but training, funding, legal, and regulatory considerations.

This publication focuses on community concerns, privacy, and civil rights issues, which from the beginning must be factored into the decisions, policies, and procedures to implement this technology. People must believe that drone usage not only will make them safer, but that the equipment will not make it easier to violate their civil liberties—or crash into their homes. Communicating these messages requires transparency about the risks and efforts to reduce them, as well as collaboration with civic organizations, other public safety agencies, and the local media.

Drones can perform search and rescue operations in much less time than ground-based teams and provide enhanced situational awareness during dangerous operations. Despite these tactical benefits, the public is very wary of them, with widespread worry about "spying," unwanted surveillance, and misuse of data collection, as well as safety concerns during flight. The COPS Office hopes that this handbook will assist law enforcement agencies and the communities they serve in making informed, collaborative plans for the use of the UAS technology.

Sincerely,

Ronald L. Davis
Director
Office of Community Oriented Policing Services

Acknowledgements

This report was made possible through the leadership of the Office of Community Oriented Policing Services, U.S. Department of Justice, particularly from Ronald L. Davis, Director; Debra R. Cohen-McCullough, former Senior Social Science Analyst; Deborah L. Spence, Supervisory Social Science Analyst; and John H. Kim, Social Science Analyst.

The Police Foundation would like to recognize that this work would also not have been possible without the cooperation of the Arlington (TX) Police Department, especially Chief Will Johnson, and the Mesa County (CO) Sheriff's Office, especially Benjamin Miller, the former Quartermaster and Unmanned Aircraft Program Director. Both agencies provided numerous documents and expertise to help ensure the accuracy of this guidebook. The Police Foundation also provides special recognition to Anne T. McKenna, Esq. formerly of SilverMcKenna and currently Visiting Assistant Professor of Law at Penn State Law, who prepared the extensive legal analyses that appear in the appendices of this guidebook.

A special thanks must be given to the numerous participants of the five regional focus groups who provided invaluable expertise and insights into the potential use of unmanned aircraft systems by law enforcement. It cannot be emphasized enough how instrumental their insights were to the development of this guidebook.

- Chief Bryan Roberts, Draper City (Utah) Police Department, Midwest Regional Focus Group
- Chief (Ret.) Scott Seaman, Los Gatos (California) Police Department, Northern California/West Coast Regional Focus Group
- Chief (Ret.) Jim Burack, Milliken (Colorado) Police Department, Mountain Regional Focus Group
- Detective Lieutenant Stuart Greer, Morristown (New Jersey) Police Department, Mid-Atlantic Regional Focus Group
- Sheriff (Ret.) Rod Hoops, San Bernardino (California) Sheriff's Department, Southern California/West Coast Regional Focus Group

Additionally, the Police Foundation would like to recognize the following individuals who served on the advisory board for this project for their invaluable expertise, insights, and commentary during the advisory board meeting held in June 2014 and throughout the writing process:

- Mr. Douglas Bodrero, President, Institute for Intergovernmental Research, Tallahassee, Florida
- Mr. Paul Brooks, former CEO/Executive Director, Chantilly, Virginia
- Mr. Earl Cook, Chief, Alexandria Police Department, Alexandria, Virginia
- Mr. Ken Corney, Chief, Ventura Police Department, Ventura, California
- Ms. Ayn Crawley, Director, Office of Civil Rights and Civil Liberties, U.S. Department of Homeland Security, Washington, DC
- Mr. Michael German, Fellow, Brennan Center for Justice, New York University, New York City, New York
- Mr. Thomas Hicks, Chief Programs & Technology Officer and Assistant Executive Director, International Association of Fire Chiefs, Fairfax, Virginia
- Mr. Steve Ingley, former Executive Director, Airborne Law Enforcement Association, Frederick, Maryland
- Mr. Will Johnson, Chief, Arlington Police Department, Arlington, Texas

- Mr. Thomas Manger, Chief, Montgomery County Police Department, Montgomery County, Maryland
- Mr. Benjamin Miller, former Quartermaster, Mesa County Sheriff's Office, Mesa, Colorado
- Mr. David Morton, UAS Integration Office at the Federal Aviation Administration (Ret.).
- Mr. Michael O'Shea, Senior Law Enforcement Program Manager, Office of Justice Programs, U.S. Department of Justice, Washington DC
- Mr. Charles Ramsey, former Commissioner, Philadelphia Police Department, Philadelphia, Pennsylvania
- Mr. Donald Roby, Captain (Ret.), Baltimore County Police Department, Baltimore County, Maryland and former Chair, Aviation Committee, International Association of Chiefs of Police, Alexandria, Virginia
- Mr. Henry P. Stawinski, Chief, Prince George's County Police Department, Prince George's County, Maryland
- Mr. Darrell Stephens, Executive Director, Major Cities Chiefs Association, Charlotte, North Carolina
- Mr. Edwin Roessler, Jr., Colonel, Chief of Police, Fairfax County Police Department, Fairfax County, Virginia
- Mr. Charles Werner, Chief (Ret.), Albemarle County Fire Department, Albemarle County, Virginia

Furthermore, we would also like to recognize the following individuals for their participation in the advisory board meeting held in June 2014:

- Joo Y. Chung, former Director, U.S. Department of Justice, Office of Privacy and Civil Liberties, Washington DC
- Mr. Timothy Field, Second Lieutenant, Fairfax County Police Department, Fairfax County, Virginia
- Ms. Dianne Gittins, Deputy Chief, Alexandria Police Department, Alexandria, Virginia
- Ms. Amy Kurren, Senior Counsel, U.S. Department of Justice, Office of the Associate Attorney General., Washington DC
- Mr. Steve Pansky, Senior Air Traffic Control Analyst, Science Applications International Corporation (SAIC) supporting the Federal Aviation Administration Unmanned Aircraft Systems Tactical Operations Section, Washington DC
- Mr. Daniel Schwarzbach, former Executive Director/CEO Airborne Law Enforcement Association, Frederick, Maryland
- Mr. Chris Wundrach, Captain, Oakland County Sheriff's Office, Oakland, Michigan

In particular, we would like to especially thank Mr. Field, Mr. Miller, Mr. Roby, and Mr. Pansky for their insightful and constructive comments on drafts of the guidebook.

The development of this guide and creation of this report were led by the following members of the Police Foundation project team: James Bueermann, President; Maria Valdovinos, Research Associate; and James Specht, former Police Foundation Communications Manager, with support from Clifford Karchmer, former Police Foundation Consultant and Fellow; Mary Sigler, former Police Foundation Project Associate; Adam Kaufman, former Police Foundation Research Assistant; and Saniya Seera, former Police Foundation Intern. A special thanks to Blake Norton, Vice President/ Chief Operating Officer; James Burch, Vice President, Strategic Initiatives; Don Shinnamon, Police Foundation Executive Fellow; and Jennifer Zeunik, Director of Programs, for their insightful reviews and assistance in the writing, vetting, and formatting of this guidebook.

Executive Summary

There is no question that technology is rapidly changing the face of policing today. Most police forces now have computers in patrol cars and communicate with their officers via cell phone. They actively use new technologies to gather license plate data and pinpoint hot spots of crime. New DNA testing capabilities are reopening thousands of old cases, offering the chance to complete an investigation or, in some cases, reverse a wrongful conviction.

A driving force among cutting-edge businesses is the search for "disruptive" technologies—a product that will completely transform a market and potentially make former products obsolete. Technology has been a "disruptive" force for law enforcement in many ways. For example, the use of cellphone cameras and the explosive growth of body-worn cameras have irreversibly changed the nature of policing.

Like these other technological breakthroughs, the development of small unmanned aircraft systems (sUAS) has the potential to revolutionize policing. These systems are portable, relatively easy to learn and use, and are becoming increasingly affordable as more manufacturers enter the growing market.

The agencies that have pioneered the use of this technology have discovered that a sUAS can increase operational efficiency and improve officer and community safety. They can, among other benefits, help find lost persons, protect police officers during searches for armed suspects, decrease time needed to process crime and accident scenes, and aid in disaster relief and recovery.

But this is just the start.

Developers have already produced prototype miniature unmanned systems that can be carried in a pocket. They are perfecting the ability of sUAS to fly through a building using their own GPS systems. They are increasing battery power to enable them to fly longer distances or hover in place for an hour or more. And we can only imagine that the use of this technology could one day be the "Airborne Partner" to every public safety officer regardless of their location or the situation they are confronted with.

The potential for these systems has caused a number of policing agencies to take note. However, early adopters of this new technology have discovered a painful truth: Where law enforcement leaders see a wonderful new tool for controlling crime and increasing public safety, a portion of the public sees the potential for a massive invasion of privacy. In the public mind the type specimen of unmanned aircraft systems is the military drone, able to hover for days, spying indiscriminately and conducting missile strikes without warning.

Furthermore, the regulatory environment in the past allowed hobbyists to buy and fly sUAS the same day, while law enforcement leaders faced a number of challenges to using this relatively new technology. Chief among those were restrictions placed on sUAS use by the Federal Aviation Administration (FAA). As a result, few police and sheriff's departments completed the rigorous authorization process and received approval for use. However, in August 2016 the FAA completed an eight-year rulemaking process and established regulations to allow the use of sUAS in the National Airspace System (NAS). With the regulatory framework in place, the use of sUAS will undoubtedly grow at a much greater pace.

In addition, numerous privacy advocates and concerned citizens, as well as state legislatures across the country, have strong and valid concerns regarding privacy and safety. For example, at least 17 states have placed some level of restriction on police use of sUAS, and many others have legislation under consideration. The concerns and questions are many, and the answers thus far, are few.

The President's Task Force on 21st Century Policing (2015) notes that technology can indeed, be a double-edged sword for law enforcement. While it can provide immeasurable benefits, it can also cause police officers to spend less time interacting with citizens. The resulting alienation can cause communities to see law enforcement as an occupying force, completely divorced from the concerns of the public.

To avoid this alienation, the task force recommended increased engagement with the community during the acquisition phase of any new technology. As task force co-chair and former Philadelphia Police Commissioner Charles Ramsey noted: "Just having the conversation can increase trust and legitimacy and help departments make better decisions."

Law enforcement agencies considering adopting a sUAS must consider ways to include and engage their community in the decision-making process. Beyond official restrictions, law enforcement agencies across the country have encountered strong public opposition when purchasing a sUAS. Protests over potential police surveillance of citizens have led some departments to shelve their sUAS before they ever used them. The public outcry has made it clear that if law enforcement is to benefit from sUAS use, they must involve the community in the process, being transparent on the benefits and risks and on the safeguards that will be put in place to protect public privacy and safety. Strong community relationships and communication can ensure that sUAS become community assets used to solve community problems.

Understanding the challenges these public perceptions of sUAS bring, the Police Foundation, in partnership with the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS), has developed this guidebook to help public safety agencies successfully assess the appropriateness of acquiring a sUAS in their jurisdiction, all the while ensuring public support, avoiding public-relations pitfalls, and enhancing community trust along the way.

As this guidebook outlines, the acquisition of a sUAS provides police with another opportunity to increase outreach and engagement with their communities. The agencies that have succeeded in acquiring a sUAS for their departments have undertaken community-focused outreach such as meeting with skeptics, and have provided repeated public demonstrations of the capabilities of their sUAS.

The recommendations laid out in this guidebook— maximizing transparency, engaging the community, and proactively developing privacy-protection protocols— have the potential to become a positive "disruptive" force in police practices: a force that transforms former practices. Following this successful formula could be the first step toward making community policing practices the watchword in the policing of the future.

I – Background

The combination of greater operational flexibility, lower capital requirements, and lower operating costs could allow UAS to be a transformative technology in the commercial and private sectors for fields as diverse as urban infrastructure management, farming, and disaster response. Although these opportunities will enhance American economic competitiveness, our nation must be mindful of the potential implications for privacy, civil rights, and civil liberties.

– **President Barack Obama**,
"Promoting Economic Competitiveness
While Safeguarding Privacy, Civil Rights, and Civil Liberties
in Domestic Use of Unmanned Aircraft Systems."

Law enforcement agencies across the nation are considering the benefits of adding a small unmanned aircraft system (sUAS) to their force. Beyond official restrictions, the main challenges states and law enforcement face have little to do with technological capabilities and much to do with complex issues surrounding the collection of data and potential violations of privacy. To address these issues, law enforcement agencies considering adopting a sUAS must also consider ways to include and engage their communities in the decision-making process. Recognizing the complexity of these decisions , the U.S. Department of Justice's Office of Community Oriented Policing Services (COPS) sought to create a guidebook for law enforcement that would offer an overview of the technological benefits of a sUAS, potential, legal challenges and liability issues, and strategies for community engagement.

Police Foundation/COPS Office Community Policing and UAS Project

With support and funding from the COPS Office, the Police Foundation developed this guidebook in concert with law enforcement executives and community representatives from across the U.S. It includes practical recommendations for engaging the community in a conversation about a potential sUAS program; navigating the official and public obstacles to introducing a sUAS; and communicating successfully about the program. Our focus in this guidebook is specifically on small unmanned aircraft systems,[1] those weighing 55 pounds or less.

Input to the guidebook was provided by the law enforcement, public, and UAS expert communities in two main formats[2]:

1. Regional Focus Groups: Focus groups composed of law enforcement and community representatives from five jurisdictions around the country (Los Gatos, CA; Draper City, UT; San Bernardino, CA; Milliken, CO; and Morristown, NJ) met to provide perspective on sUAS deployment by law enforcement. The goal of these focus groups was to obtain both law enforcement and community input on how police can best engage their communities to build consensus while exploring the suitability of sUAS acquisition and deployment for their jurisdictions. Focus group sites were chosen

1. A small unmanned aircraft system (sUAS) is a small version of a UAS, weighing no more than 55 pounds. This is generally the type of aircraft system considered by law enforcement for public safety use. Throughout this guidebook, we have taken great effort to ensure our terminology is as consistent as possible; however, there will be places where UAS and sUAS terms are used interchangeably. It is also important to note that while the terms drone, unmanned aircraft vehicle (UAV), and unmanned aircraft system (UAS) are also often used interchangeably, there are distinctions. In this guidebook, we use the Federal Aviation Administration's definition of the UAS as consisting of the aircraft itself and all of the associated support equipment, control station, data links, telemetry, communications, and navigation equipment necessary to operate it.

2. In addition to focus group and advisory board input on the key challenges and potential benefits around this issue, the evidence base for this guidebook consists of extensive legal research, case studies, and UAS/UAV-related publications, including law review articles, peer-reviewed sources, and a variety of media sources. See the "Notes on Research Methods" appendix for more detail on the research methods used in this project.

for their diversity, not only in the composition of the communities and community groups in the jurisdiction but also in geography—for example, we expected that the concerns of communities and law enforcement agencies in urban jurisdictions would be different from those of suburban and rural jurisdictions. To obtain well-rounded input, we selected the jurisdictions for our focus groups according to the following three criteria:

1) A confirmed interest in learning the requirements for implementing a sUAS program;

2) A record of adopting technological innovations through COPS Office funding;

3) A commitment to issuing policies and procedures to structure police discretion.

2. National Advisory Board: The Police Foundation gathered together a diverse group of subject matter experts and stakeholders in law enforcement, aviation, law, and civil rights in Washington, D.C. in 2014. The advisory board included representatives of law enforcement agencies that have successfully acquired sUAS. These agencies are the Arlington (TX) Police Department and the Mesa County (CO) Sheriff's Office. Also included were representatives from several law enforcement and fire agencies and associations interested in issues associated with sUAS acquisition. Additionally, the advisory board included representatives from the Federal Aviation Administration (FAA), National Institute of Justice (NIJ), Department of Homeland Security (DHS), and the Brennan Center for Justice at NYU Law School to provide insight into the relationship between new technology and privacy issues. At the 2014 meeting, the advisory board conducted an environmental scan of the issues related to law enforcement use of sUAS.[3]

In this guidebook, law enforcement will find blueprints for determining whether their community could benefit from a sUAS, building dialogue around sUAS acquisition with the community, co-producing public safety, and operating a sUAS program with transparency. Section I outlines basic information on UAS technology; its evolution; its benefits and challenges to law enforcement; conducting cost-benefit research; and where community policing and sUAS use intersect. Section II provides an overview of legal and regulatory constraints inherent in sUAS use, including constitutional law; state legislation; FAA regulations; and community concerns and liability. Section III walks the reader through conducting a needs assessment process, including engaging the community and developing an operating plan. Section IV reviews steps in sUAS program planning: developing program policy, staffing and training, and engaging the community and the media. Finally, Section V discusses program implementation; impact evaluation; and community engagement throughout the life of the sUAS program. The guidebook also contains a wealth of resources and informational materials in the links and appendices, including examples of ways to educate and inform the public about sUAS and ways to inform community organizations, city councils, and state legislatures about expectations of privacy and law enforcement use when lawfully deployed.

The purpose of this guidebook is to provide law enforcement agencies with an overview of the potential costs and benefits of using UAS, legal challenges and liability issues, and impact on privacy and community trust. It uses community policing principles to guide agencies on ways to proactively and effectively engage their community on the issue, develop operating plans to protect safety and privacy, and create a legal framework for the successful deployment of a sUAS as an additional tool in the co-production and enhancement of public safety and the fight against crime. Chapter 1 begins this discussion by introducing the role of community-oriented policing principles in helping law enforcement leaders navigate the rocky terrain of this issue.

3. An organization's participation on the advisory board should not be interpreted as an organizational endorsement of the entirety of this report or its recommendations.

CHAPTER 1

Community Policing and UAS

Unmanned aircraft systems (UAS), specifically small unmanned aircraft systems (sUAS), have the potential to greatly enhance law enforcement operations. From search and rescue to accident scene investigation to protecting officer safety in active shooter situations, sUAS offer a wide range of potential operational improvements. However, law enforcement agencies interested in leveraging UAS technology in their departments must consider the needs, fears and concerns of their communities. Community concern regarding potential police surveillance of citizens can thwart efforts to implement sUAS programs and force departments to ground their sUAS before they ever get to fly them.

Focus group and advisory board members urge agencies to understand privacy laws and develop working plans informed by community policing principles and focused on the benefits to the community and officer safety, rather than on how a sUAS might be used as a law enforcement tool.

Community policing derives from the concept that trust and mutual respect between police and the communities they serve is critical to public safety. Officially defined, community policing is a philosophy that promotes organizational strategies that support the systemic use of partnerships and problem-solving techniques to proactively address the immediate conditions that give rise to public safety issues such as crime (COPS Office 2012). Law enforcement agencies around the country have spent decades working to strengthen community relationships by building their departments' culture on community policing philosophies and practices, such as transparency, community engagement, and strong communication. When considering implementation of new, potentially controversial technology, it is important for police departments to rely on these practices, and engage the community in decision-making and implementation.

The importance of community input can be learned from situations where police agencies have bought a sUAS without carefully planning and involving their community. Consider these three recent cases:

- The Seattle Police Department (NBC News 2013) purchased two unmanned aircraft systems with funds provided by the U.S. Department of Homeland Security. Public outcry over the possibility of their use for spying and other privacy concerns led the mayor to cancel the program before the sUAS ever flew.
- The San Jose Police Department (San Jose Police Department 2014) purchased sUAS with Homeland Security funds, and began to put together a plan to use them. The public learned of the purchase, and through public outcry and newspaper editorials (Herhold 2014) clamored for them to be returned.
- The Los Angeles Police Department (Serna 2014), which received the banished Seattle sUAS as a donation, was forced to state publicly that it had no plans to use them for the foreseeable future.

At the same time, as use of small unmanned aircraft systems by community members for professional and personal purposes continues to expand, law enforcement is increasingly called upon to respond to incidents involving them. From simple trespassing complaints, to more dangerous problems like flying near manned aircraft or over-crowded public events, to outright criminal use, law enforcement agencies are having to develop innovative ways to respond to the use of sUAS by some individuals, while protecting the safety and rights of all.

Many law enforcement executives are left wondering if UAS and Community Policing can peacefully coexist, and if so, how. The following are only some of the questions to be addressed:

- How can UAS deployment affect community trust in the police, and what can the police do to uphold that trust?
- How can police use sUAS for life-saving missions while maintaining their commitment to procedural justice, transparency, and accountability?
- How can police agencies balance the benefit of using UAS for surveillance in targeted public safety missions with real or perceived threats to privacy within the community?
- What technological and operational considerations should police consider before deployment?
- "What are the primary community apprehensions that police are likely to encounter when planning for and deploying UAS, and how can they best address them?" (Cohen McCullough 2014)
- What data will be captured by sUAS during use, and what laws govern its collection, use, dissemination, destruction, or public release?

Successful deployment of a sUAS program is predicated on the ability of law enforcement to balance the benefits of the technology with the preservation of community privacy, safety, and other concerns. Agencies must weigh the potential civil liabilities that may arise from UAS use and establish robust guidelines to prevent misuse that could potentially harm existing relationships with the community.

It is critical for agencies to involve and engage the community throughout the entire sUAS implementation process in an effort to sustain trust and continue to build police legitimacy. The strength of a department's relationship with its community is an important determinant of whether a sUAS program can be implemented successfully.

Summary

Community policing derives from the concept that trust and mutual respect between police and the communities they serve is critical to public safety. Building on community-oriented policing principles of transparency and police-community cooperation gives law enforcement leaders a vehicle to navigate rocky terrain, while continuing to build trust with the community regarding the potential establishment of a sUAS program. It is critical for agencies to involve and engage their communities throughout the entire process, from the first point of consideration onward.

Research, the establishment of policy in the deployment and utilization of the technology, and appropriate training are all key to implementation of any new technology. The following chapters present an overview of the basics of UAS technology—its terminology, history and evolution—as well as benefits and challenges. These chapters are intended to serve as a foundation for agencies interested in sUAS.

CHAPTER 2

UAS Terms and Technology

UAS technology

The long-standing official Department of Defense (DoD) term for 'drones' is *unmanned aerial vehicle* (UAV), defined as powered aircraft that do not have an onboard crew (DoD 2001). The FAA defines (FAA 2013) these vehicles as *unmanned aircraft* (UA), described as all winged aircraft and helicopter-type aircraft of any size that do not have onboard pilots. An *unmanned aircraft system* (UAS) includes the UA and the technology and crew to fly it. Under the FAA definition, this may include control stations (ground-, ship-, or air-based), control links, support equipment, payloads, flight termination systems, and launch/recovery equipment.

Due to cost constraints, law enforcement agencies typically use unmanned aircraft systems that weigh no more than 55 pounds.[4] These are part of the group defined by the agency and the unmanned aircraft industry as *small unmanned aircraft systems* (sUAS). The most popular sUAS are small vertical-lift aircraft that are lightweight and easily transported but have enough power to carry a high-quality camera, a sensor package and a technology package that can include a global positioning system (GPS), allowing the aircraft to be programmed to fly a route without remote pilot control. Operating with an onboard stability system, the aircraft can hover over one area for an extended period and provide high-quality video and, with the proper equipment, infrared images. Importantly, if the link is lost between the unmanned aircraft and the pilot in command (ground control station), the failsafe systems are designed to either return the sUAS or land it in place.

There is wide variation in the designs and capabilities of sUAS. Generally, however, quadcopters (with four rotors) are the least expensive and easiest to repair. Hexacopters (with six rotors) and octocopters (with eight rotors) are more powerful and can carry a heavier payload, but are more expensive. The one major drawback of the small copter-style sUAS is their relatively short flying time. Most have a battery life of 20–30 minutes or less, although the hexacopters and octocopters can be equipped with a larger battery.

sUAS features

Although they can vary greatly in price, the sUAS marketed to law enforcement agencies include the following basic features:

- **Portability**, allowing the sUAS to be folded up or quickly taken apart and stored in a hard case that fits into the trunk of a vehicle. The case also includes space for the controller, one payload camera, battery chargers, and some spare parts like extra rotors. Some models also provide a separate backpack for field use.
- **Ground controller**, including a screen to receive video images, a solid-state transmitter with antenna to communicate with the sUAS, and some configuration of joystick controls. Some ground controllers include a detachable screen (Draganfly 2015b) that allows for separate controls of video cameras. Others allow tablets or smart phones (Draganfly 2015d) to be connected to receive the video image.
- A fully integrated **avionics controller** on the sUAS, including a GPS system and a receiver/transmitter to communicate with the ground station. The software package includes a failsafe system that alerts the operator in case of low battery or if the unit is close to its range or height limit. If the link to the ground controller is lost, the failsafe systems are designed to either send the sUAS into an automatic return flight or slowly land the sUAS in place. Many manufacturers are now including software that allows a set route to be programmed, allowing the sUAS to fly without ground controls using GPS coordinates.

4. The FAA will issue approval of a UAS weighing more than 55 pounds; however, the operations of that UAS may require additional provisions as part of the approval.

- A basic **payload package** that includes a color video/still camera and an infrared camera. Many systems now have these cameras combined for one payload (Falcon Unmanned 2015). Most sUAS have a quick release or plug-and-play gimbal system[5] that allows rapid changes in payloads and maintains image stability while in flight.

PROHIBITIONS AGAINST WEAPONS ON UAS | Both the FAA General Operating Rules, and the International Association of Chiefs of Police (IACP) Recommended Guidelines for Use of Unmanned Aircraft prohibit the use of weapons of any sort on unmanned aircraft.

Because most sUAS are designed with the plug-and-play easy installation systems, watchdog groups like the American Civil Liberties Union (ACLU) have predicted that a number of potential payloads could be added in the future, including environmental sensors to detect hazardous materials, "see-through" radar imaging, video analytics like license plate readers, and electronic surveillance capabilities that could collect cell phone metadata (Stanley and Crump 2011).[6]

As law enforcement agencies consider the acquisition of a small unmanned aircraft system, it is important to maintain transparency about the intended use of the sUAS and how any additional payload capacity will contribute to the improvement of officer safety and public benefit. Specific information about the intended use of all payload technology should be provided to policy-makers and the community.

Choosing a sUAS

In 2011, the U.S. Department of Homeland Security Science and Technology created the Robotic Aircraft for Public Safety (RAPS) testing system, which has evaluated commercial sUAS at a testing site near Fort Sill in Oklahoma (Divis 2013). More than 70 companies submitted aircraft to be tested, with 50 accepted into the program. The agency is in its second phase of testing, including GPS and other sensor systems.

The RAPS testing system found that hovering types of sUAS—known as quadcopters, hexacopters and octocopters—provide the best performance for operations like urban search and rescue, accident scene reconstruction, and finding the location of a hidden suspect, as well as aiding in arson investigations and urban disaster relief. Fixed wing sUAS can fly longer and may be better for search and rescue in remote areas, the study found (Appleby 2013).

Most comparisons of sUAS performance to other methods have been to manned aviation units, with a large focus on the cost savings produced by UAS over manned aviation. While performance metrics (i.e. time) for UAS versus other methods are not widely available in a standardized format, increased public safety use of these systems will provide for easier comparisons, allowing for benchmarking of performance.

FOCUS ON THE FIELD | The Arlington (TX) Police Department has purchased two sUAS: a Leptron Avenger sUAS, designed as a small version of a traditional helicopter, which can be equipped with a larger battery and can fly in 40 mph winds; and, more recently, a Leptron Rapidly Deployable Aerial Surveillance System (RDASS) to survey storm damage.

The Mesa County (CO) Sheriff's Office has acquired a Falcon UAV fixed-wing sUAS that can also fly for longer periods, approximately 20–40 minutes longer than most other sUAS currently used by law enforcement (table 1).

Law enforcement agencies can also access the reviews of the various systems through the System Assessment and Validation for Emergency Responders (SAVER) Program, accessible through the FirstResponder.gov website. Reviews are proprietary and only available to law enforcement agencies that register with the SAVER system.

5. A gimbal is a pivoted support that allows the rotation of an object about a single axis. Gimbals are used for stabilization and balanced movement.

6. The dropping or spraying of aircraft stores or carrying of hazardous materials outside of restricted, prohibited, or warning areas approved for these types of aviation activities is prohibited unless specifically authorized as a special provision.

Table 1: Comparison of sUAS currently used by law enforcement agencies

	Draganflyer X6	AeroVironment Qube	Falcon Hover	Falcon	Phantom 3
Type	Vertical takeoff hexacopter	Vertical takeoff quadcopter	Vertical takeoff quadcopter	Fixed-wing, bungee cord launch	Vertical takeoff quadcopter
Size	34x34 inches	18x36 inches	48 inches tip to tip span assembled	8 feet x 4 feet assembled	23 inches diagonal assembled
Weight	2.2 pounds	5 pounds	5 pounds	9 pounds	2.8 pounds
Payload capacity	2.2 pounds	2 pounds	2 pounds	2 pounds	2.8 pounds
Flying time	20–25 minutes	40 minutes	20+ minutes	60+ minutes	20–25 minutes
Camera available	Sony QX 100 20.1 megapixel 3.6x optical zoom	High-resolution camera/IR combination	Combination day/ IR video camera; Sony Nex7 24.3 MP Forward down-look	Combination day/ IR video camera; Sony Nex7 24.3 MP Forward down-look	Sony Exmor 1/2.3" effective pixels: 12.4 M (total pixels: 12.76 M)
Ground system	Handheld controller can be split	Rugged touchscreen tablet	Laptop control station, powered by car battery	Laptop control station, powered by car battery	Advanced handheld remote controller
Infrared camera	Purchased separately	High-resolution camera/IR combination	Combination day/ IR video camera	Combination day/ IR video camera	Purchased separately
Cost	$21,000 with infrared camera	$50,000 complete	$8,000–$16,000* base	$12,000–$24,000* base	$699–$1,259 base

Source: Manufacturers – Draganfly.com; Falcon.com; avinc.com; DJI.

* According to the Falcon Unmanned website, a minimum of 2 aircraft of the same type is required per purchase.

Evolving technology

Interest and investment in UAS technology has reached a fever pitch. UAS companies continue to innovate, driving down cost and expanding UAS capability. Because of this, more and more individuals, companies, and government organizations are identifying ways to leverage UAS benefits; and the trend does not appear to be slowing. UAS technology continues to mature in a number of ways.

- **Cost**: sUAS, which just a few years ago cost $5,000 or more, can now be purchased for under $1,000, complete with a high definition camera mounted on a gyroscopic platform and a battery that will last from 30–60 minutes. The most recent models include a GIS-based autonomous flying system that can pilot the sUAS through a set course without being controlled by a human operator.
- **Capability**: sUAS capability continues to expand every day. To date, some are able to hover with a takeoff weight of 50 pounds or more (Altigator 2015), hover 400 feet above a street, view an entire city block at a resolution showing details of yards and rooftops, or fly at speeds up to 50 mph.
- **Development**: sUAS technology advancement is driven by an open-source community that freely shares innovations through websites such as DIYdrones.com and takes full advantage of 3D printers. Sharing and rapid prototyping have facilitated the

creation of new ways to carry payloads and of methods to protect rotors and keep the sUAS flying even after collisions with walls (or other sUAS) (Koller 2014, Coptaire 2011).

- **Quality**: The FAA predicted in 2013 that there would be 7,500 commercial UAS in U.S. airspace within five years. The agency later revised that estimate to reflect that there may be 10,000 in the air by 2017 (FAA 2014b). Developers and the 'drone community' predict there could be that many private sUAS in the air by the time the FAA releases its guidelines.[7]

Usage of the terms drone, UAS, and sUAS

It is frustrating to many enthusiasts of unmanned aircraft systems that the media and most of the public insist on calling everything that flies without a pilot a drone. The concern is intensified by the fact that the term drone has become associated with large military-style weapons like the Predator that have been repeatedly used for stealthy—and increasingly controversial—attacks on targets in the Middle East and Pakistan. Magazine covers like Time Magazine's February 11, 2013 illustration for "The Rise of the Drones," showing a menacing Predator hovering over homes, are indicative of the public's perception of drones as militaristic fighting machines in the sky—a major obstacle to law enforcement's ability to convince the public that their department's sUAS program could actually increase public safety, not jeopardize it. These images have led many law enforcement agencies to go out of their way to avoid the use of the word "drone" in reference to their sUAS.

FOCUS ON THE FIELD | Arlington (TX) Police Chief Will Johnson has found that allowing the community to view the sUAS during community meetings has greatly helped to ease concerns and has helped to convey how different these systems are from the Predator type drones used by the DoD.

Leaders in departments that have been successful in creating a sUAS unit say there is no way to avoid the term in conversations with the public. However, the FAA advises that its preferred term for these aircraft is unmanned aircraft system (UAS), which takes into account not only the unmanned aircraft (UA) itself but also the data link, the attached sensor(s), the navigation system, and the ground control station (FAA 2015b).

Members of the Police Foundation focus groups stressed that law enforcement leaders should accept that the public is going to use the term drone and should make an effort to explain how the systems they plan to use are dramatically different from the Predator and other systems used by the DoD. While most media stories have focused on the Predator and other larger military UAS that can carry maximum payloads upwards of 4,000 pounds and travel at maximum speeds of 300 miles per hour for periods of 20–30 hours (Collinson 2011),[8] this is a very specific type of UAS design for a very specific type of military operation. As can be seen in this chapter, the types of UAS currently used by and marketed to law enforcement agencies are much smaller in scale and limited in capability than military drones.

For purposes of this guidebook, the term Unmanned Aircraft System (UAS) or small Unmanned Aircraft System (sUAS) will be used instead of the term drone whenever possible.

7. Congress had tasked the FAA with a deadline of September 2015 to create regulations allowing commercial UAS into public airspace, but the agency has admitted it is behind schedule.

8. The features summarized here are typical of MQ-9 system designs and were pulled from a description of the features of an MQ-9 system.

Summary

The FAA defines *unmanned aircraft* (UA) as all winged aircraft and helicopter-type aircraft that do not have onboard pilots. An unmanned aircraft system (UAS) refers to the aircraft and all of the associated support equipment, control station, data links, telemetry, communications, and navigation equipment necessary to operate it. Small unmanned *aircraft systems* (sUAS) are small versions that weigh 55 pounds or less.

Although there is a wide variation of designs and capabilities for sUAS, most are relatively inexpensive, portable, and have a number of capabilities particularly well suited for law enforcement operations, which has led to a growing market for this technology for public safety use. As law enforcement agencies consider the acquisition of an unmanned aircraft system, it is important to maintain transparency about what the intended use of the sUAS will be, and how any additional payload capacity will contribute to the improvement of officer safety and public benefit. Specific information should be provided to policy-makers and the community about how all payload technology will be used.

Chapter 3 presents an abbreviated overview of the history and evolution of UAS technology.

CHAPTER 3

Evolution of UAS

Military use of UAS

The U.S. military began extensive use of the UAV[9] during World War II, when "radio-planes" were flown to provide practice targets for anti-aircraft gun operators. The military continued to refine these vehicles, and by the 1960s, was making efforts to create unmanned surveillance aircraft to conduct missions to document Chinese nuclear facilities. The development of the Predator UAV in the 1990s, and its success in the war in Bosnia, led the DoD to dramatically increase funding committed to the development of military UAVs. By 2015, more than 50 unmanned aircraft vehicles of various sizes were under production and being considered by branches of the military.

The Army and Navy have also acquired a large supply of smaller, hand-launched unmanned aircraft for field operations and troop support.[10] It is this type of small unmanned aircraft that has increasingly come to the attention of law enforcement. Police and public safety organizations are drawn to the sUAS by the same advantages that attracted military attention: ease of training, portability, and the ability to gain a view of the terrain ahead without putting personnel at risk.

Both members of Police Foundation regional focus groups and the national advisory board have pointed out that law enforcement's use of UAS developed on the battlefield may heighten public concerns that adoption of this technology is another example of the increasing militarization of police agencies. It is incumbent upon law enforcement agencies to make the distinction between military and civilian unmanned aircraft and to strengthen advocacy of this position; that is, that while their functions and benefits may be similar, the sUAS used for public safety are **not** military drones.

In chapter 2 we provide a comprehensive overview of the types of sUAS as well as features currently marketed to law enforcement.

Commercial use of UAS

UAS technology continues to evolve, spurring exponentially-increased use in communities across the country. The market for domestic sUAS—considered toys just a few years ago—could grow by more than $13 billion over the next three years if the FAA allows them to become integrated into commercial airspace, according to the Association for Unmanned Vehicle Systems International (AUVSI), the main industry trade group (AUVSI 2013). This increase has market implications that span not only revenue generation and improved capability, but also potential employment opportunities for properly trained and experienced UAS operators.

Among the varied commercial markets that stand to benefit from sUAS are agriculture, energy, utilities, mining, construction, real estate, news media, and film production (AUVSI 2013). As photography and video platforms, sUAS can provide unique vantage points on infrastructure such as reservoirs, stadiums, and bridges (Yakabe 2015), without the safety risks of using crewed aircraft or of sending photographers and surveyors into dangerous areas. Safety is often cited by commercial users as one of the major benefits of sUAS use, along with the increasing sophistication and affordability of the equipment (Yakabe 2015).

Additionally, wide aerial surveys of entire crop fields, installations, and sites facilitated by sUAS can increase not only site safety but also revenue

9. The DoD refers to unmanned aircraft as "vehicles" whereas the FAA refers to these aircraft as "systems."

10. Armed forces from around the world have acquired more than 13,000 of the AeroVironment Raven Q11, a hand-launched UAS that weighs 2 pounds and is about 4 feet long. Other popular models include the RQ12 "Wasp," a smaller UAS designed to resemble a bird in flight. The Army put in nearly 150,000 combat hours in one year with the Raven UAS, primarily for "over-the-horizon" or urban street reconnaissance.

potential, by allowing for exceptionally accurate measurement of property lines as well as tracking of progress (Soaring Sky 2015). The American Farm Bureau Federation (Measure 2015) has found that sUAS can help measure the health of crops across an entire field, map terrain for field drainage, and aid in insurance claims for crop damage.

COMMERCIAL GROWTH | AUVSI reports that among the first 500 FAA commercial use applications, requested uses included the following:

- **Real estate, 153**
- **General aerial surveying, 128**
- **General aerial photography, 125**
- **Agriculture, 106**
- **Construction, 74**
- **Utility inspection, 69**
- **Film and television, 65**

(Some applications requested multiple uses.)

Though recreational uses of sUAS range as widely as do the personal and recreational interests of the hobbyists and operators who use them, photography and videography are among the most often cited recreational uses. As long as the images captured are for personal use and not compensation or sale, hobbyists are not required to obtain approval from the FAA to fly, but are subject only to certain technical and safety guidelines.

For commercial markets, the low cost of sUAS combined with the wide range of uses is credited with driving the significant growth rate seen in the last couple of years. This rate is anticipated to continue to increase in the upcoming years, not only because of the continuing and increasing demand for the technology but also because of the potential employment opportunities it provides. The FAA began granting exemptions for commercial use in May 2014, and had only approved seven by September 2014. However, according to the AUVSI, by July 2015, the FAA had approved more than 1,500 commercial applications for sUAS use (AUVSI 2015). As of November 2015, approvals total over 2,200 (FAA 2016).

As a result of the significant growth seen since 2014, Congress tasked the FAA with a deadline of September 2015 to create regulations allowing commercial UAS into public airspace.

After an eight-year rulemaking process, the FAA established Part 107 – SMALL UNMANNED AIRCRAFT SYSTEMS in August 2016 as part of the Code of Federal Regulations (FAA 2016d). Part 107 allows use of sUAS weighing less than 55 pounds in certain airspace during daylight hours only, within line of sight of the pilot and no higher than 400 feet above ground level (AGL). Further, the air vehicle may not be flown over any persons not directly participating in the use of the system. The regulations also establish Remote Pilot in Command certification and responsibilities.

Summary

Unmanned aircraft vehicles and systems have a long military history extending back to World War II. Both members of Police Foundation regional focus groups and the national advisory board have pointed out that law enforcement's use of UAS developed on the battlefield may heighten public concerns that adoption of this technology is another example of the increasing militarization of police agencies.

Although law enforcement use of sUAS has faced challenges, commercial and private use of the technology has grown exponentially. The demand for access to the National Airspace System (NAS) led to the FAA establishing the regulatory framework necessary for safe integration of unmanned aircraft.

In chapter 4 we present the findings of our cost-benefit research on UAS technology.

CHAPTER 4

UAS Cost-Benefit Research

Cost-benefit research

Law enforcement agencies exploring the suitability of a sUAS for departmental operations must thoroughly explore costs and benefits. The relatively low cost of sUAS technology and operations, when compared to manned technology and operations, makes it an attractive alternative for departments that are looking to increase service while maintaining or even cutting back operational budgets. However, because departmental costs vary from agency to agency, and because so few law enforcement agencies are currently operating sUAS on a regular basis, it is difficult to develop a concise, easily monetized cost-benefit analysis. Adding to the complexity, some of the most significant benefits of a sUAS are in increased officer and public safety, where a monetary value is difficult or impossible to assign. In these cases, assumptions and approximations may need to be made to make appropriate comparisons. In this chapter, we provide an overview of cost considerations that a department should take into account in researching UAS.

Comparing manned and unmanned aircraft units

Many law enforcement agencies measure the costs of using a UAS against the costs of a fully manned aviation unit (Sherman 2015), such as a helicopter, in an effort to analyze UAS costs and benefits. The Mesa County Sheriff's Office determined that a sUAS could perform about 30 percent of the functions of a manned system (Miller 2013), while the Arlington (Texas) Police Department estimated a sUAS could perform as much as 80 percent of the everyday operations of a manned aircraft, according to Chief Will Johnson. However, both agreed that the cost to run the sUAS would be less than 10 percent that of a manned system.

Manned aviation units can cost millions of dollars a year to operate, compared to an operating cost of a few thousand for unmanned aircraft systems. The Mesa County Sheriff's Office reports that since 2008 they have spent a total of $14,000 in operation costs at approximately $25/hour.

In addition to basic cost savings over manned aviation, a sUAS can be carried in the trunk of a police cruiser and requires little space for storage. Maintenance is light and can be performed by the operator, and repair costs are easily manageable—in some cases, the entire sUAS unit can be replaced for the cost of engine maintenance on a manned aircraft.

The cost difference between a law enforcement helicopter and a small unmanned aircraft system can be dramatic:

- Acquisition cost: Helicopter, $600,000–$1 million; sUAS, $12,000–$40,000 (Repard 2015)
- Operating cost for fuel and maintenance: Helicopter, $245–$600/hour; sUAS, $25/hour (Repard 2015, Valenzuela 2014)
- Housing/Storage: Helicopter $300–$500/month; sUAS, none (most fit in a vehicle trunk) (Sherman 2015)

Personnel costs have also been difficult to determine because most departments that have created sUAS units have cross-trained existing officers, many of whom have continued to perform other duties in addition to operating the sUAS. Both Mesa County and Arlington have created four-person teams that include a pilot, an observer, a video operator, and a supervisor who acts as a liaison with other law enforcement and with local air traffic controllers.

Training costs include $3,000 to $5,000 for a 40-hour pilot's license course, with a two-day training course for sUAS operation provided at about $2,000 by the manufacturers. Other costs include the initial and ongoing training required for the agency to comply with FAA regulations, or self-certify the sUAS team as a public aircraft operator. Self-certification, depending on the level of aviation

experience the agency possesses, can be the more expensive option.

Another cost to consider—one that has not been well established for sUAS—is insurance cost. While an annual insurance plan for a law enforcement helicopter can be $30,000 a year, much of that is predicated on the potential for loss of life of both the pilots and those on the ground in case of an accident. While a sUAS weighing about five pounds still has the potential to cause injury, the risk is smaller. Additionally, insurance analysts report that insurance rates can be reduced (Wright 2015) for law enforcement sUAS flown by certified pilots and operators. The Arlington Police Department's 2015–2016 year insurance premium totaled $4,017.00 (APD Aviation Unit, personal communication, February 17, 2016).

Comparing costs based on mission

Another way to compare the costs and benefits of using a sUAS is to research the costs of conducting law enforcement missions with and without sUAS. For example, the following chart outlines costs associated with using no aviation, a manned helicopter, and a sUAS in search and rescue and incident reconstruction missions.

Tools for conducting UAS cost-benefit research

While building UAS cost-benefit research can be a tedious process of identifying, comparing, and documenting associated costs and benefits, tools do exist to assist in the effort. One advisory board member recommends using the *Technology Decision Tool* developed by the National Law Enforcement and Corrections Technology Center (NLECTC). The tool "guides agencies through a customized cost/benefit analysis exercise to help them make the best decisions for their officers and their communities" (JustNet 2016).

Cost-benefit research of UAS acquisition and operation will vary from jurisdiction to jurisdiction, but is a critical component of any needs assessment process. An overview of UAS cost-effectiveness considerations can be found in appendix 1.

Cultivating funding for UAS acquisition

To date, every law enforcement agency that has reported acquiring a sUAS has used grants from the U.S. Department of Homeland Security to cover the costs of the new technology. The Homeland Security Grant Program (DHS 2015b) includes two funding streams that have been used by local agencies to acquire a UAS: The State Homeland Security Program and the Urban Areas Security Initiative (UASI). Both of these programs are administered through state homeland security agencies. While the grant programs have been reduced in recent years, Congress approved $600 million for UASI and $350 million for the State Homeland Security Program for Fiscal Year 2015.

Purchase costs for sUAS have fallen dramatically as production and sales increase, resulting in some advanced models that can be acquired

Table 2. Summary of cost comparison

	No aviation	Manned helicopter	sUAS
Acquisition	N/A	$600,000–$1 million	$12,000–60,000
Operating cost (w/o personnel)	N/A	$245–$600/hour	$25/hour
Personnel	N/A	5–10 member crew	3–5 member crew
Search and Rescue (100-acre field)	100 resource hours	5–10 minutes	5–10 minutes
Incident reconstruction	3–5 resource hours	1–2 person-hours	1–2 person-hours

by private individuals for as little as $2,500 (DJI 2015). As the technology continues to improve and prices continue to fall, law enforcement agencies will find it easier to consider purchasing a UAS using operating funds or through donations from police foundations and other support groups.

FOCUS ON THE FIELD | Arlington Police Chief Will Johnson said his department explained the purchase of a sUAS using a business model: how much could be saved, what uses would most promote officer and public safety, and what capabilities would a sUAS provide that couldn't be obtained otherwise.

Regardless of how the technology is funded, law enforcement sUAS purchases require support from the community and policy-makers, emphasizing the need for outreach and engagement prior to sUAS acquisition. The most successful cost-benefit research plans will involve the community and key stakeholders in determining how the sUAS will be used to benefit the community.

Summary

Law enforcement agencies exploring the suitability of a sUAS for departmental operations must thoroughly explore the costs and benefits. Compared to manned aviation, sUAS offer significant cost savings due to their small size and light maintenance. Because departmental costs vary from agency to agency, and because so few law enforcement agencies are currently operating sUAS on a regular basis, it is difficult to develop a concise, easily monetized cost-benefit analysis; however, cost-benefit research is an important part of a needs assessment for any law enforcement agency considering acquisition of a sUAS. In this chapter, we provide an overview of cost considerations that a department should take into account in researching UAS.

In Chapter 5 we further explore the benefits and challenges of law enforcement's use of sUAS.

CHAPTER 5

UAS and Law Enforcement

Police-community partnerships

Today, more than ever, law enforcement agencies are seeking ways to build and advance relationships with community partners to solve community problems. While new technologies may be divisive, their introduction can also lead to community consensus and the enhancement of trust, when it is approached under the guidance of the community policing principles of transparency and police-community cooperation. Assessing the community's need for a sUAS program and implementing it as a community safety asset can be a way for law enforcement agencies to develop partnerships for promoting public safety.

A WORD FROM THE FOCUS GROUP | "The community is more willing to accept the technology if they have an awareness of UAS and an understanding of what they are and their capabilities."

– Focus Group Participant

Benefits of UAS

While UAS may provide a number of possible crime control capabilities, as a community asset, the sUAS has the potential to improve both community and officer safety, while decreasing the cost of improved operations. It can even save lives, as the following examples illustrate:

- **Improving Search and Rescue Operations**. The ability of sUAS to maneuver in relatively small and difficult-to-access areas makes it a promising technology to assist with search and rescue operations. Some law enforcement agencies, such as the Royal Canadian Mounted Police (RCMP 2013), as well as private groups, have used sUAS to help locate individuals with special needs or disabilities. One sUAS hobbyist located a lost senior citizen (BBC 2014) in a field in 20 minutes after a three-day search with dogs and hundreds of volunteers failed to find him. In a recent missing person case, Virginia Tech also used a sUAS in their search and recovery efforts for missing student Hannah Graham. UAS may not be able to replace manned aviation units entirely, however, as battery life and legal restrictions such as line of sight requirements may limit their effective use.
- **Protecting Officer Safety**. Some departments use sUAS to get a better look at suspicious packages or locate hidden (and possibly dangerous) suspects while reducing risk to officers. Grand Forks County Sheriff's deputies used a Qube, a small 5.5 lb. aircraft system with four rotor blades, to track four suspects fleeing a DUI stop in approximately half an hour, safeguarding the deputies from having to give chase into a cornfield with stalks measuring 7 to 10 feet high (Stone 2014, Fox Business 2014). Focus group members noted that many agencies already do this with bomb-disposal robots, but the sUAS could be in action sooner and make a much quicker sweep of the scene. For arrests, a sUAS could provide overhead views of both front and back doors, potentially improving officer safety. When executing search warrants, sUAS can provide a broad display of the property (this is especially helpful for illegal marijuana farms on public land, police say).

FOCUS ON THE FIELD | Arlington (TX) Police Department identified the following recent events in the city of Arlington that benefited from the use of sUAS: Super Bowl XLV (security, visual inspection of roof); motorcycle accident at night on New York and I-20 (location of rider thrown from bike); crime scene of missing elderly person; 50-vehicle pileup on I-20; flooding at Pioneer Parkway and Park Springs.

sUAS can also be used to improve the operational capacity and efficiency of law enforcement tasks, providing officers with situational awareness and location information:

- **Accident and Crime Scene Investigations**: An aerial survey by a sUAS, particularly one equipped with GIS mapping software, can save hours in follow-up investigations. This can speed up accident and crime scene investigation and report preparation and may reduce incidental traffic associated with a scene investigation. The RCMP has reported (Cape Breton Post 2014) increased accuracy and efficiency in using sUAS for accident reconstructions (Draganfly 2015c). The Mesa County (CO) Sheriff's Office has used a sUAS in an increasing number of crime scene investigations (Miller 2013).
- **Disaster Management**: sUAS can survey damage in flooded or inaccessible areas (Envisage Technologies 2014) quickly, saving responders vital time and protecting their safety. Relief workers have already used sUAS to assess remote villages after Philippine typhoons (Santos 2013) and to determine the instability of buildings after the earthquake in Haiti, according to the United Nations Office for Coordination of Humanitarian Affairs (OCHA 2014).
- **Perimeter Security**: sUAS can provide views of hard-to-access areas (Lerner 2014), improving officer and public safety. This can be crucial in securing areas before public events as well as in border protection. For example, the Ohio Department of Rehabilitation and Correction plans to use unmanned aircraft systems to watch the perimeter of its prisons (Ohio DOT 2014).
- **Active Pursuit Support**: Focus group members noted that using sUAS to follow fleeing suspects, particularly when they are on foot, protects officer safety, and could also reduce the danger to the public. Indeed, some agencies (such as Grand Forks, mentioned previously) have used their sUAS in pursuit situations. It is important to note, however, that under current FAA guidelines, a department sUAS crew must have uninterrupted visual sight of the sUAS throughout the pursuit, making sUAS assistance in vehicle pursuits unlikely (FAA 2015d).

Finally, some agencies with sUAS programs suggest considering purchasing the technology as a *shared community resource*, providing mutual aid to other government agencies:

- **Support and Coordination with Fire/ EMS and Other Government Agencies**: While some advisory board and focus group participants warned against it (due to the confusion of command and control), some believe entering into a mutual aid agreement with local fire, EMS, or other government agencies to acquire and use a sUAS could be beneficial to the community. Firefighter safety could be greatly improved by the use of a sUAS to view roof damage during a fire. Additionally, public works, community development, parks and recreation, environmental work (such as mosquito control), transportation (like mapping evacuation routes), planning, and many other public responsibilities could benefit from implementation of UAS technology.

As the use of this technology in police departments continues to increase across the country, driven by improvements in technology and reductions to cost, identification of more public safety uses for UAS will likely occur. Careful consideration of community and departmental needs and how UAS technology can assist in filling those needs should drive technology implementation decisions. Law enforcement agencies should devise strategies to open lines of communication regarding how implementation of sUAS programs will address community needs. These strategies should begin from the onset of serious consideration of a sUAS program, and should ensure two-way communication: that is, law enforcement agencies must be able to inform the public of their needs and consideration of new technology to address those needs, and the community must be able to pose questions, voice concerns, and make suggestions, secure in the knowledge that they will be heard and their own needs addressed. In this way, introduction of new technology (such as UAS) can present opportunities for law enforcement to initiate positive non-enforcement engagement with

their communities, and provide opportunities to solve community challenges (such as those posed by introduction of UAS) in a collaborative manner.

Challenges in implementation

While the potential benefits of UAS use by law enforcement are numerous, challenges also exist with implementation of this new technology. Law enforcement agencies interested in leveraging the benefits should also be prepared to address all competing concerns and potential liabilities. Among these are the following:

- **Regulations**: The regulatory environment in the past made legal operation of a sUAS by law enforcement agencies challenging. While hobbyists could buy and fly sUAS the same day,[11] law enforcement users faced many obstacles to using unmanned aircraft, most notably the FAA policies restricting their use. As a result, few police and sheriff's departments completed the rigorous authorization process and received approval for use. For example, by 2014, only a handful of agencies had begun flying UAS after receiving a Certificate of Authorization (COA) from the FAA (FAA 2014a). However, in August 2016 the FAA established regulations to allow the use of sUAS in the NAS. With the regulatory framework in place, the use of sUAS will undoubtedly grow at a much greater pace.
- **Community Concerns**: Ensuring that the community understands, is involved in, and trusts law enforcement intentions for sUAS use will be an ongoing process. Well-publicized policies and procedures safeguarding the legal and safe use of UAS in the community and detailing the oversight mechanisms that will ensure accountability will be paramount.
- **Technology and its Use in its Infancy**: Use of UAS in public air space is a relatively new phenomenon. Even in preparing this guidebook, examples and best practices were sometimes difficult to come by because so few agencies are using sUAS in law enforcement operations. It is simply unexplored territory. As the field progresses, however, more lessons will be learned that can guide appropriate and effective UAS usage while protecting the privacy and civil liberties of the law abiding public.
- **Legal and Constitutional Considerations**: Perhaps the biggest community concern police will come across is the potential violation of privacy and Fourth Amendment rights. Law enforcement should also be cautious about using UAS to monitor political protests and other First Amendment protected public gatherings.
- **Liability**: Use of UAS in domestic airspace does pose risks of injury to persons (including physical injury and civil rights violations) and property. Law enforcement agencies are accountable to their communities for all instances of use, and must minimize risk to mitigate liability and avoid civil liability.

Responding to increased use of UAS in the community

Although commercial UAS have been allowed on a limited basis by the FAA under what were called "333 Exemptions" (in reference to Section 333 of the FAA Modernization and Reform Act of 2012, which authorized the FAA to allow for such use), and to a greater extent under the new Part 107, private, commercial, and public entities alike are becoming increasingly aware of the opportunities sUAS bring and the legal context in which they are operated. Law enforcement executives who participated in focus groups led by the Police Foundation said they are especially concerned about the potential for ill-intended people, criminals, and criminal organizations to use UAS. They urge law enforcement executives to prepare themselves and their agencies to deal with enforcement problems (Goodman 2013) even if they are not considering getting a sUAS for their department.

In January 2015, the accidental crash landing of a sUAS on the White House grounds caused a media uproar, and raised serious questions (Norton

11. In December 2015 the FAA published an interim final rule requiring sUAS to be registered. This was in response to increased reports of unauthorized and potentially unsafe UAS operations, which rose to almost 1,200 in 2015. Aircraft registration provides an immediate and direct opportunity to hold users accountable for noncompliance with safe operating requirements.

2015) about the ability of the United States Secret Service and other law enforcement agencies to track and stop sUAS that might fly into restricted airspace or be used for an illegal or threatening purpose. The incident is just one of the latest of many that have caused law enforcement leaders to realize that they must pay attention to the problems, and potential threats, posed by sUAS.

Consider these widely reported incidents:

- **Seattle, WA**: Visitors to the Space Needle were startled to see a small UAS flying outside (Nicks and Grossman 2014). Some said it crashed into the window. Police traced the UAS back to a hotel room, where the operator was apparently an employee of Amazon (which has plans for order delivery by unmanned aircraft) (Amazon.com 2015).
- **Los Angeles, CA**: The LAPD has asked the City Attorney to determine whether it can legally prohibit UAS operators from flying directly over police stations (Serna 2014). They fear that such flights will provide insights into operations that are currently shielded from public view for officer safety reasons.
- **Columbia, SC**: A small UAS was found crashed just outside the perimeter fence (Kinnard 2014) at a South Carolina maximum-security prison. It was carrying marijuana, cigarettes and cell phones.
- **San Diego, CA**: A small UAS carrying methamphetamine crashed in Tijuana near the U.S. border. The incident cast a spotlight on reports that Mexican drug cartels are reportedly buying UAS to evade border security (Lopez 2014) with shipments of high-value narcotics.
- **Dresden, GDR**: German Chancellor Angela Merkel was speaking at an event when a small UAS flew in over the crowd. Everyone—including her security—watched as the buzzing UAS flew right up to the stage and landed in front of Merkel (Bittel 2013). Police observers have pointed out that the UAS could have easily carried enough explosives to devastate the entire stage.

On March 18, 2015, Chief Richard Beary, President of the International Association of Chiefs of Police (IACP) testified in front of the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, United States House of Representatives regarding the impact of proliferation of use of UAS by the general public. He pointed out that increased use of UAS by the public poses a "grave threat" to public safety. According to Chief Beary:

"Thankfully, at this point, most of the incidents involving UAS have not led to horrific events, but I don't think we are far away from seeing more incidents involving unmanned aerial systems that lead to tragedy. The concerns out there are real. There is nothing to stop the criminal element from purchasing a UAS and using it to cause localized or catastrophic damage."

Chief Beary went on to ask federal government partners to provide concise guidance on the appropriate response for law enforcement to take in response to incidents involving UAS used for criminal activity. Currently, limited guidance on response to UAS use by the public is available to law enforcement agencies. The FAA website provides two resources, the Law Enforcement Guidance for Suspected Unauthorized UAS Operations (FAA 2015c) and information on UAS use during sporting events (FAA 2014d). The former document warns that the proliferation of unmanned aircraft will require local agencies to increasingly be called on to deal with illegal activity (see Appendix 9).

While some jurisdictions have responded by creating 'no drone zones' to contain some public use of UAS, the FAA asks that law enforcement responding to complaints about potentially illegal UAS usage do the following:

- Identify potential witnesses and conduct initial interviews
- Contact the suspected operators of the UAS or model aircraft
- View and record the location of the event
- Collect evidence

- Identify if the UAS operation was in a sensitive location, event or activity
- Notify one of the FAA's Regional Operation Centers about the operation as soon as possible

Summary

Understanding the basics of UAS technology and terminology; its evolution; how UAS technology can work with community policing; the costs versus the benefits; and the challenges of its use for law enforcement provides a foundation for determining if the technology is a good fit for your community. This section has provided some of that information for law enforcement organizations interested in utilizing UAS technology as a public safety tool in their community. While UAS technology and its integration into public air space is in its infancy and details are continually evolving, we have provided the most up to date information available.

Research is critical to the needs assessment, planning, and implementation stages of any law enforcement sUAS program. Laying the legal groundwork for use, proactively addressing community concerns regarding privacy, and following the necessary steps for FAA approval will prove key in increasing initial community acceptance and implementation success. Law enforcement agencies can increase acceptance by creating transparent policies and procedures, ensuring the ability to evaluate program impact, and maintaining communication with the community.

Section II provides an overview of the legal and liability issues that should be researched by law enforcement agencies considering adding a sUAS program to their departments. In addition, Exhibit 1-A provides a checklist to guide law enforcement agencies considering implementing a sUAS program in their community. More detailed information on each of the steps can be found in the chapters that follow.

II – Legal and Regulatory Analysis

Disclaimer: The following is a brief overview of the legal issues that should be further researched by law enforcement agencies considering a sUAS. Extensive legal memoranda on the subject can be found in Appendix 11 of this guidebook. Law enforcement agencies are strongly advised to consult with their own City Attorney or District Attorney on legal and constitutional issues surrounding the use of unmanned aircraft systems before launching their program. While the legal issues surrounding UAS use are rapidly evolving as the courts consider them, significant guidance can be found in existing constitutional law addressing other technologies.

CHAPTER 6

Constitutional Law

Before law enforcement leaders begin to use any new technology, one important factor to consider is whether the technology will raise legal and constitutional issues. This is particularly important in addressing law enforcement use of UAS technology in a community-policing environment. As with numerous other technologies, the use of UAS is evolving much quicker than the law. However, a logical place to start when analyzing the UAS legal environment is constitutional protection.

THE RXP TEST | When interpreting the Fourth Amendment right to privacy, courts consider whether citizens have a reasonable expectation of privacy (RXP) in the situation. People on city streets do not have an RXP, but they do have an RXP in their homes. When considering UAS use in open spaces, consider whether people have a reasonable expectation of privacy (RXP) in this space.

The Fourth Amendment to the United States Constitution prohibits unreasonable search and seizure. It is explicitly recognized that the Fourth Amendment protects people, and not places. As such, people must have a reasonable expectation of privacy (RXP) in certain spaces such as in their homes, and in public spaces configured and provided to ensure privacy. For example, in Katz v. United States (1967), the Court held that attaching a listening device to a public telephone booth violates the Fourth Amendment. In United States v. Knotts (1983), the Court ruled that a person travelling on a public thoroughfare does not have a reasonable expectation of privacy in his movement from one place to another. More recently, in United States v. Jones (2012) the Court ruled that the law enforcement action of attaching a GPS device to a car without a warrant not only constituted an unlawful search in violation of the Fourth Amendment but also a trespass into a constitutionally protected area, thereby highlighting the ability of certain technologies to intrude without actual physical trespass.

Another means to analyze the legality of UAS use by law enforcement is to review the types of technological devices that can be found on an unmanned aircraft system, and apply corresponding Fourth Amendment jurisprudence.

1. Cameras (still and video), which are primary UAS payload, are subject to the same standards, laws and restrictions that govern their manual use, or use when they are attached to helicopters or street-lights. Courts have held that anything that can be viewed by a person standing in a public space does not fit the standard for RXP, and so is not subject to Fourth Amendment protection. A person walking on a sidewalk or the outside of a car or building can be viewed. However, courts have ruled in other cases that video provided by an elevated camera may be considered an invasion of privacy. If an officer in a public space cannot obtain the view provided by the UAS, a warrant is required.

2. One of the main public concerns is the potential for intrusion that may be posed by unmanned aircraft that are equipped with surveillance cameras or video recording equipment. These devices, mounted on a UAS may allow for the collection of images that might otherwise require trespass. An example of this would be a fenced backyard. While in California v. Ciraolo (1986) the Supreme Court ruled that there was not a Fourth Amendment violation when officers took photographs of a private residence while flying at 1000 feet, and in Florida v. Riley (1989) the Court ruled once again, that photographs of a private residence taken while flying at 400 feet did not constitute a search, these spaces are not public spaces and as such, it is strongly advised that law enforcement obtain a warrant when using a sUAS to conduct targeted surveillance of a suspect's property.

3. GPS devices on a UAS, and the GPS evidence gathered via the UAS, will generally be governed by the same statutes and case law as traditional electronic tracking devices. In United States v. Knotts (1983), the Court ruled that law enforcement did not violate the Fourth Amendment when they attached a tracking beeper to a container of chloroform with the owner's consent prior to it being taken by the defendant. But in United States v. Karo (1984), the court ruled that turning on the beeper did constitute a search, and thus required a warrant.

4. The concept of reasonable expectation of privacy, and thus the RXP test, will frequently lead law enforcement to what is often referred to as "the firm but bright line of privacy at the door of the home." This line, along with the Kyllo v. United States (2001) decision, provides law enforcement with significant guidance regarding the use of thermal imaging devices commonly available for installation and use on UAS. That guidance is easily summed in three words: seek a warrant.

5. Data interception. Under the recent ruling in Joffe v. Google (2013), police who use a sUAS to intercept and collect unencrypted or encrypted WiFi data without a warrant are engaging in wiretapping in violation of the Electronic Communications Privacy Act.

6. Bio surveillance systems on a sUAS provide law enforcement with another set of means to safeguard the public. With sensors to detect radiation and other chemicals, these systems are an excellent tool for officers to obtain situational awareness in the event of a nuclear accident or terrorist attack. There have not been any serious challenges to the use of these technologies in the courts.

N.Y. V. CLASS (1986) | Because the exterior of an automobile is for all intents and purposes in the public eye, it may be visually examined by police without a warrant.

UNITED STATES V. CUEVAS-SANCHEZ (1987) | Video surveillance of private property from a pole camera, when obtained without a warrant, constitutes a search in violation of the Fourth Amendment.

KYLLO V. UNITED STATES (2001) | Warrantless use of a thermal imaging device on a private residence constitutes a search that violates a person's right to privacy.

The Police Foundation focus groups found significant community support for public safety functions of sUAS (as opposed to crime control), highlighting the numerous activities undertaken by police that could potentially pose a safety risk for both officers and the public. Among these, search and rescue operations and disaster management both pose significant potential hazards to officer safety. Additionally, firefighter safety could be greatly improved by the use of an unmanned system to view roof damage during a fire, for example. Perimeter security for large scale events, such as a football game or parade, also pose signficant public safety considerations, for which sUAS have been found to provide significant benefits. These are important points to keep in mind when communicating information to the public regarding the intended departmental use of the sUAS.

CASE GUIDANCE ON DIFFERENT TYPES OF SURVEILLANCE

- **Were communications intercepted? If so, wiretapping statutes may apply**
- **GPS tracking (see *U.S.* v. *Jones*)**
- **Images taken (see *Dow* cases)**
- **Thermal imaging capabilities on board (see *Kyllo* v. *U.S.*)**

While courts have not fully considered the legality of police use of sUAS for surveillance, court decisions on other technologies can guide law enforcement in the use of sUAS. Many states and localities are considering laws and regulations that would require a warrant for any law enforcement use of a sUAS. Among the subject matter advice offered at the advisory board meeting was to look at the specific technology used for data acquisition. "Look at what the technology is

when you are making data acquisition, and if it requires a warrant traditionally, then it also requires a warrant when it is on a UAV," said Anne T. McKenna, Esq., a Police Foundation consultant and attorney formerly with Silver McKenna, the Internet and privacy law group of Silverman, Thompson, Slutkin & White, LLC.

This means that law enforcement leaders don't have to become experts on new case law to use sUAS, but they do have to understand and apply the laws and limits that they already operate under with other practices or technologies. Also, they should inform their communities about this legal review and what it means for UAS use. To this end, police should answer these questions with regard to sUAS use:

- What is the overall purpose of information collected?
- What does law enforcement intend to do with the information collected?
- How will law enforcement ensure that the information is properly stored (in line with both legal requirements and retention policies) and/or destroyed?

The main guidance from the patchwork of case law presented here can be summed up simply: "Just because you can does not mean you should." The use of sUAS enhanced with technology by law enforcement to engage in audio and visual surveillance of activities occurring in a private home would be just as unconstitutional as in other traditional cases. This point should be emphasized to community members along with the assurance that such unauthorized use is not deemed acceptable by law enforcement. In public spaces, and in those gray spaces, it is important to always use the RXP test as a starting point to guide decision-making regarding UAS use. More detailed legal analysis (legal memoranda) can be found in Appendix 11 of this report.

Summary

As with numerous other technologies, the use of UAS is evolving much quicker than the law. While courts have not yet fully considered the legality of police use of UAS for surveillance, court decisions on other technologies can guide law enforcement in the use of sUAS. Another means to analyze the legality of UAS use by law enforcement is to review the types of technological devices that can be found on a sUAS, such as a video recording device, and apply corresponding Fourth Amendment jurisprudence.

This chapter has presented a brief overview of the constitutional protections and legal issues that should be further researched by law enforcement agencies prior to sUAS acquisition. Extensive legal memoranda on the subject can be found in Appendix 11 of this report; however, it is strongly advised that departments obtain appropriate legal guidance from their city attorney or district attorney, given the complexity and rapidly evolving nature of the issues surrounding the use of UAS. In Chapter 7 we present the current legislative landscape.

CHAPTER 7

State Legislation[12]

Public opinion on whether law enforcement agencies should be able to use UAS has wavered, but the negative reaction to the potential invasion of privacy is strong. An Iowa state poll (Petroski 2014) supports this: 76 percent of the respondents fear the loss of privacy and believe UAS should only be used when approved by a warrant. Most public and legislative concern about UAS has centered on privacy and civil rights: Will they be used to spy on citizens in their homes?

In 2013, states began introducing UAS legislation in a rapid-fire fashion. This reaction reflected a fear held by the public that UAS were going to begin collecting information and spying on them, and that this technology needed to be tightly regulated. According to the National Conference of State Legislatures, in 2013, 43 states introduced 130 bills and resolutions addressing UAS issues (NCSL 2015a). By year's end, only 13 of these states had enacted any laws. In 2014, 35 states considered UAS and/or UAV bills and resolutions and 10 states successfully enacted new laws (NCSL 2014b). These states are Alaska, Illinois, Indiana, Iowa, Louisiana, North Carolina, Ohio, Tennessee, Utah, and Wisconsin. In 2015, 45 states considered 166 bills related to UAS, and 26 of these states have so far enacted laws (NCSL 2016). An additional 38 states have considered bills related to UAS in the 2016 legislative session, with 15 states passing legislation in support of UAS technology development (NCSL 2016). Appendix 2 contains a reference list of enacted UAS legislation to date.

Much of this earlier legislation deals with defining what a drone is and what it is not, and limiting law enforcement's ability to gather information or evidence. New laws that require a warrant for UAS use in information gathering—with varying emergency exceptions—are on the books in Alaska, Florida, Idaho, Illinois, Indiana, Iowa, Montana, North Carolina, Oregon, Tennessee, Texas, Utah, Virginia, and Wisconsin. Emergency exceptions are allowed for national security; emergency response for safety, search and rescue; and crime scene and traffic crash scene photography. There are some other permissible uses, however. Oregon HB 2710 allows UAS use for training purposes. Texas HB 912 allows police to use UAS for information gathering and documentation at a crime scene where an offense greater than a misdemeanor has occurred. Such warrant exceptions, which are not related to emergency or national security response, are rare. More recent legislation has begun to address use by the general public and regulations for use in hunting.

Illinois appears to have the most comprehensive and regulatory law with regard to how data collected through a UAS may be used and maintained. The legislation (SB 1587), called

STATES WITH ENACTED UAS LEGISLATION (2013–2015)

- Alaska
- Arkansas
- California
- Florida
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Louisiana
- Maine
- Maryland
- Michigan
- Mississippi
- Montana
- Nevada
- New Hampshire
- North Carolina
- North Dakota
- Ohio
- Oregon
- Tennessee
- Texas
- Utah
- Virginia
- West Virginia
- Wisconsin

12. While copies of the state legislation referenced in this chapter are not included with the guidebook, a state legislation chart is summarized in Appendix 2 and is also included as part of the legal memoranda in Appendix 11. Because new state legislation is continually being enacted it is important to periodically visit sites such as the National Conference of State Legislatures for the most up-to-date information.

the Freedom from Drone and Surveillance Act, provides a detailed blueprint on data retention and disclosure for law enforcement in Illinois. Utah SB 167 also addresses data retention, disclosure, and reporting to a comprehensive degree. In 2014, Alaska joined this short list of states addressing the regulation of data retention through HB 255.

CURRENTLY ENACTED UAS LEGISLATION APPLICABLE TO POLICE

- **Alaska (HB 255)**
- **Florida (SB 92)**
- **Idaho (SB 1134)**
- **Illinois (SB 1587, HB 1652, and SB 2937)**
- **Indiana (HB 1009)**
- **Iowa (HF 2289)**
- **Louisiana (HB 1029)**
- **Maine (LD 25)**
- **Montana (SB 196)**
- **Nevada (AB 239)**
- **North Carolina (SB 402 and SB 744)**
- **Oregon (HB 2710 and HB 4066)**
- **Tennessee (SB 796, HB 1952, and SB 1777)**
- **Texas (HB 912 and HCR 217)**
- **Utah (SB 167 and HB 296)**
- **Vermont (SB 155)**
- **Virginia (HB 2012, SB 1331, HB 2125, and SB 1301)**
- **Wisconsin (AB 203 and SB 196)**

Sources: McKenna 2014c, NCSL 2016.

Admissibility has been addressed to a greater degree than data disclosure, retention, and reporting. Appendix 2 lists the states that have addressed admissibility requirements. The rule regarding admissibility is simple: the courts will consider as inadmissible any information gathered by police using a UAS in violation of the law and/or without a search warrant.

Summary

In 2013, states began introducing UAS legislation in a rapid-fire fashion. This reaction reflected a fear in the public that UAS were going to begin collecting information and spying on the public, and that this technology needed to be tightly regulated. Much of this legislation deals with defining drones and limiting law enforcement's ability to gather information or evidence with them. More recently, legislation has begun to address use by the general public. Illinois appears to have the most comprehensive and regulatory law with regard to how data collected through a UAS may be used and maintained. Admissibility has been addressed to a greater degree than data disclosure, retention, and reporting. Chapter 8 provides an overview of current Federal Aviation Administration regulations addressing UAS.

CHAPTER 8

Federal Aviation Administration Regulations

The mission of the Federal Aviation Administration (FAA) is to provide for the safety and efficiency of the National Airspace System (NAS). Integrating rapidly evolving unmanned aircraft technology into the NAS has proven challenging. Since the mid-2000's, the FAA has regulated unmanned aircraft operations by using policy documents, while it went through the process to develop actual regulations. In accordance with FAA policy, public agencies that wanted to operate a sUAS were required to obtain a Certificate of Authorization or Waiver (COA) from them. The COA process was lengthy and required civil airman testing and in some cases certification, airworthiness declarations, operational policies, etc. While it appeared to be cumbersome, it did require the public agency to properly develop its UAS program in order to assure the safety of the NAS.

After an eight-year rulemaking process, the FAA established Part 107 – SMALL UNMANNED AIRCRAFT SYSTEMS in August 2016 as part of the Code of Federal Regulations (FAA 2016d). The new regulations only apply to "civil" sUAS operations. The question that will be faced by many law enforcement agencies, most of them unfamiliar with aviation operations, is whether to conduct operations as a "civil" aircraft and comply with the new Part 107, or as a "public" aircraft and seek a COA from the FAA.

The Code of Federal Regulations (14 CFR Part 1) defines two types of aircraft, civil and public. In general terms, public aircraft are those owned and operated by the United States Government or the government of a state or a political subdivision of a state. Public aircraft used for *commercial purposes* change their status to that of civil aircraft. Status depends on the type of operation the aircraft is conducting at the time rather than the aircraft itself.

Civil aircraft are simply defined as anything other than public aircraft.

The regulatory difference between civil and public aircraft is significant. In essence, public aircraft are statutorily exempt from most types of FAA regulation, including civil airworthiness and airman certification. For example, 14 CFR Part 61.3 states that a person may not act as pilot in command of a **civil** aircraft unless that person has a valid pilot certificate. Pilots of public aircraft are **not** required to hold an FAA-issued pilot certificate. Public aircraft are, however, subject to the airspace and air traffic rules of Part 91 of 14 CFR.

With Part 107 now in place, the public agency has a choice to either voluntarily operate as a civil aircraft, or continue to obtain a COA from the FAA and operate as a public aircraft.

The requirements of Part 107 include the following:

- **Operational limitations:**
  - Applies to sUAS that weigh less than 55 lbs. (25 kg)
  - The aircraft must remain within visual line of sight of the pilot
  - May not be operated over any person not directly participating in the operation
  - Is restricted to daylight operations only
  - Does not require the use of a visual observer
  - Can fly at a maximum altitude of 400 feet above ground level (AGL)
  - Operations within Class G (uncontrolled) airspace are authorized without permission from air traffic control

- **Remote Pilot in Command (RPIC) Certification and Responsibilities:**
  - » Establishes an RPIC airman certificate
  - » The RPIC is responsible for ensuring the condition of the system is safe for operation prior to flight
- **Aircraft Requirements:**
  - » FAA airworthiness certification is not required

Compliance with Part 107 is not difficult and enables many public safety applications. Though basic, it provides a framework for an agency to develop a program, especially those just starting the process. As agencies gain experience and wish to expand to more complex operations, there is a process to get a waiver from most of the flight restrictions if the agency can demonstrate that it can be done safely. Finally, by complying with civil UAS regulations, the agency provides assurance to its *community*—which may be skeptical of the agency's ability to safely operate unmanned aircraft—that it is complying with all federal regulations for UAS operations.

As noted, should the agency decide to operate as a public aircraft, it will need to obtain a COA from the FAA. While COAs in the past required the agency to fully develop its program prior to receiving authorization to operate, post-107 COAs will only address airspace and operational limitations. The FAA has stated that it does not anticipate issuing public aircraft COAs that are less restrictive than what is contained in Part 107. The agency can request a waiver, just as in Part 107, if it can prove the operation can be done safely. Perhaps most importantly, the agency will have to self-certify its pilots. This will require them to develop their own training program, something beyond the capabilities of many agencies without extensive aviation experience.

Summary

The use of unmanned aircraft technology by law enforcement is in its early stages. As some obstacles, such as the economy, cultural resistance and regulatory issues, begin to recede, more agencies will seek to use unmanned aircraft. Regulatory compliance is just one factor in program development. Others include community engagement, funding, operational policy development, and training for pilots and other members of the sUAS team. In essence, the process to properly develop an unmanned aircraft program is very complex.

This section has, so far, provided an overview of legal, legislative and regulatory considerations for law enforcement agencies interested in using sUAS in their communities. It is incumbent on agencies to further research these considerations prior to acquisition of UAS technology in order to address specific community nuances, and to ensure accurate information is communicated to community members. The next chapter highlights some of the community and liability concerns that pose challenges for law enforcement agencies interested in sUAS.

CHAPTER 9

Community Concerns & Liability

As with almost any technology, the use of UAS poses challenges and liability risks for law enforcement. The legal and legitimacy implications of new technologies are often under-considered by law enforcement agencies prior to adoption. For example, in a national survey of police agencies that adopted license plate reader technology, only 28.5% reported having researched the legal implications of the new technology before adopting it (Lum et al 2010). While these risks cannot be eliminated in their entirety, there are proactive steps agencies can take to mitigate potential liability risks they might face.

In order for communities to be open to the use of sUAS by law enforcement, the public safety benefits of their use must clearly outweigh any potential risks. Use of sUAS in domestic airspace does pose risks of injury to persons (including physical injury and civil rights violations) and property. Law enforcement agencies are accountable to their communities for all instances of use, and must minimize risk to mitigate liability (McKenna 2014c). Law enforcement could face liability in cases of:

- **Injury to person or property**: Injury to person or property as a result of physical collision with a sUAS is subject to the same type of liability that arises from a police cruiser collision with either a person or private residence. This type of potential liability is familiar to virtually all law enforcement agencies in the United States.
- **Violations of a person's right to privacy**: Injury to a person's right to privacy due to intrusion into constitutionally protected affairs is related to the Fourth Amendment right of freedom from unreasonable search and seizure (McKenna 2014b).
- **Violations of the First Amendment:** In a directive issued May 22, 2015, the U.S. Department of Justice specifically called on federal agencies to avoid any UAS operation conducted "solely for the purpose of monitoring activities protected by the First Amendment" and other rights granted under the Constitution and federal law (DoJ 2015). The potential ability of a UAS to hover over gatherings has been cited as a potential violation of the First Amendment right to freedom of assembly (McKenna 2014c).

CIVIL RIGHTS VIOLATION | An individual who believes their Fourth Amendment rights have been violated can file a civil rights lawsuit based on 42 U.S.C. Section 1983, which permits federal suit alleging violation of constitutional or statutory right.

In order to proactively address potential liability and minimize risk, law enforcement agencies should have an understanding of how and when they could be subject to civil suits by members of their communities. Specific UAS incidents that could expose a law enforcement agency to civil liability include the following:

- **UAS collisions:** Civil liability could result from crashes and collisions due to negligent operation and maintenance, and resulting in injury or damage to persons or property (Rapp 2009).
- **Violation of property rights:** Violation of property rights could occur as a result of noise and visual nuisance. Constant and low flying sUAS in front of a landowner's property could result in civil liability based on trespass and nuisance (Great Westchester Homeowners' Assn. v City of Los Angeles 1979).
- **Interference with communication systems:** Law enforcement agencies could be subject to civil liability if members of the public suffer damages due to lost services because a sUAS interferes with cell phone, Internet, or television service (Rapp 2009, note 12).

- **Violation of a person's right to privacy**: Law enforcement surveillance using a sUAS could result in civil liability based on violations of the Fourth Amendment and the right to privacy.
- **Violations of the First Amendment:** Law enforcement agencies should prepare strict guidelines on when a sUAS might be used during political protests, and detail how First Amendment rights will be protected by policies on data gathering and use.
- **Liability based on federal statute:** For example, civil violations of the Wiretap Act and improper disclosure of collected information could also result in civil liability.

In light of the numerous potential instances of civil liability resulting from UAS use, what can law enforcement agencies do to proactively manage the risk? Key recommendations include the following:

- **Use standard operating policies and procedures:** Implementation of standard operating procedures that are applied uniformly and are followed consistently should be a first step for any agency looking to establish a sUAS program.
- **UAS program training:** Any officer involved in the operation, maintenance, and otherwise general use and control of a sUAS must undergo proper training and must obtain the appropriate certifications. This training should not be restricted to operation and maintenance of the sUAS itself. It is equally important that officers involved with a sUAS have a thorough understanding of the Fourth Amendment protections that could be potentially violated by the use of the sUAS.
- **UAS program operating procedures:** It is extremely important that detailed procedures be developed for every stage of sUAS operation, maintenance, and inspection. Agency policy should require detailed reporting and documentation of these procedures. A preflight and postflight checklist should be used to ensure that no step is missed. Although these checklists will likely differ across agencies and jurisdictions, some of the important elements that could be included are
  - preflight review of the goals and mission;
  - statement on the role each member of the sUAS team will play;
  - criteria for determining whether advance notification must be provided not only to air traffic control but also to communities;
  - a list of backup procedures to be followed in the event of loss of communication or contact;
  - a reminder of prohibited acts involving UAS.
- **UAS program oversight:** In order to minimize risk of liability as a result of use, any law enforcement sUAS program should have a system of checks and balances in place that includes procedures for auditing, system oversight, and clear consequences for misuse. Misuse could not only undermine the legitimacy of an established sUAS program, but also irreparably damage community trust in the program and the agency as a whole. Not only does misuse open the door to civil liability, it also opens the door to criminal liability for officers, supervisors, and state and local government entities.

STANDARD OPERATING PROCEDURES |
The Special Operations Standard Operating Procedure (SOP) from the Arlington (Texas) Police Department is a model of a comprehensive policy designed to "minimize risk to people, property, and aircraft during operations of the sUAS while continuing to safeguard the right to privacy of all persons." It is included in this guidebook as an additional resource.

Accountability: a key component of community policing

Measures for ensuring accountability to the community are key for any sUAS program and should be established early—well before a program is established. Assuring the community that your department will be 100% accountable for any and all use of the sUAS and the data it collects is the first step in the process of obtaining community consensus. As noted by the IACP in their technology policy framework,[13] accountability should be ensured at all levels, including sworn and civilian employees, contractors, subcontractors, and volunteers.

The exact procedures for ensuring accountability will vary from department to department, but the responsibility for carrying them out will likely rest with community policing officers and citizen advisory boards. Community policing officers carry the message of police departments to communities, accomplishing much of the work formerly undertaken by community relations units, and could incorporate messaging regarding UAS into existing work with the community. For example, the Mesa County (CO) Sheriff's Office has for several years now introduced their sUAS to the community at the annual Mesa County Safety Fair, where the sUAS team is available to showcase the aircraft, answer questions, and provide the opportunity for members of the community to see the systems up close.

Citizen advisory boards are convened across the country to provide input into law enforcement issues such as recruiting and hiring, civilian complaints, and internal investigations. Civilian oversight could be extended to accountability procedures for sUAS use. In fact, the *Final Report of the President's Task Force on 21st Century Policing* (2015) supports this type of input, recommending that "[l]aw enforcement agencies should encourage public engagement and collaboration, including the use of community advisory bodies, when developing a policy for the use of a new technology."

Summary

In order for communities to be open to the use of sUAS by law enforcement, the public safety benefits of their use must clearly outweigh any potential risks. The use of sUAS poses challenges and liability risks for law enforcement which fuel community concerns. The liability risks for law enforcement include injury to persons or property, violation of a person's right to privacy, and violations of the First Amendment, among others. Taking measures to ensure accountability to the community is key for any law enforcement sUAS program, and should be established early—well before a sUAS program is implemented. Some ways in which law enforcement agencies can work to proactively manage the risk of liability from sUAS use are establishing standard and program operating procedures, conducting program training, and ensuring sufficient program oversight.

Ensuring community input into law enforcement sUAS programs, from program inception through implementation, helps to ensure community trust and promote accountability. In section III we focus on conducting a needs assessment to determine whether UAS technology will address the needs of your community, and whether the community is ready for UAS technology.

13. The full IACP technology policy is included as an additional resource in this report.

III – Determining Whether Your Community is Ready for UAS Technology: Conducting a Needs Assessment

While many are contemplating the value of sUAS for law enforcement purposes, studies have shown (RTI International 2013) that the majority of police departments have yet to actually evaluate whether they can make good use of a sUAS. Conducting a proper needs assessment prior to purchasing a sUAS is critically important. Communities will feel safer and be more willing to accept law enforcement use of the technology if they understand law enforcement's preparedness to deal with sUAS use, to harness its benefit for community safety, to safeguard and appropriately limit the use of any data, images, or video produced, and to confront community concerns.

Across all focus groups, national advisory board recommendations, and lessons learned from the Arlington, Texas and Mesa County, Colorado experiences, this has been a consistent message. Resources to help law enforcement communicate this information, including the policies that will ensure public safety and appropriate use, will become increasingly important.

CHAPTER 10

Building Dialogue with the Community and Stakeholders

An increasing number of law enforcement agencies have been given an opportunity to acquire sUAS either through grants from the U.S. Department of Homeland Security (Sengupta 2013, DHS 201b), or by using asset forfeiture funds (WISTV 2013). However, it is important for agencies to make thoughtful consideration prior to determining if UAS technology is right for their community. While decisions to acquire new technology should always be driven by organizational mission and demonstrated need, for police departments using community policing philosophies, assessing the need for a sUAS must also start with a scan of community and stakeholder sentiment regarding the technology.

FOCUS ON THE FIELD | Arlington (TX) Police Chief Will Johnson said his agency made the rounds to every possible community group, showing off the small UAS the department planned to deploy and laying out in detail how it would be used for community and officer safety. The sessions directly confronted concerns, and laid out the department's policies to ensure privacy would be protected. In addition, they made the case for how a sUAS could save taxpayer funds. "We emphasized price, privacy, regulations and responsible deployment, and we really reduced anxiety," Johnson said.

The community's role in the sUAS program

Partnerships for problem solving are at the heart of the community policing philosophy. In community policing, problem solving is defined as "the process of engaging in the proactive and systematic examination of identified problems to develop and evaluate effective responses," and community partnerships are defined as "collaborative partnerships between the law enforcement agency and the individuals and organizations they serve to develop solutions to problems and increase trust in police" (COPS Office 2012). While there are many potential partners within any given community, building consensus about sUAS will require partnerships centered on developing solutions to problems. In identifying appropriate stakeholders with whom to forge those partnerships, it is principally important for police agencies to consider the public safety issues that are most prevalent in their community.

Potential stakeholders include community members and groups; other government agencies; lawmakers; nonprofit organizations; private businesses; and the media. Law enforcement leaders should also be sure to include the input of department personnel. Often, department personnel are overlooked as potential stakeholders, but gaining their perspective and ensuring consensus regarding UAS at all levels within the department is at least as important as ensuring consensus from the community. The success of police-community partnerships in implementing a sUAS program will greatly depend on ensuring acknowledgement of and agreement on UAS advantages, as well as acknowledgement of disadvantages and inclusion of concerns.

The alignment of organizational management, structure, personnel, and information systems to support community partnerships and proactive problem solving efforts is another key component of the community policing philosophy (COPS Office 2012). Underlying this framework of community-oriented problem-solving partnerships is the idea that not only do communities (and stakeholders) play a key role in prioritizing and addressing public safety problems, but that they should expect to play a key role. For departments, this means that there need to be mechanisms and channels of communication in place in order to facilitate this role and this type of community input. Unfortunately, because every department

is different, there is no one-size-fits-all approach. Law enforcement agencies considering the implementation of a sUAS program will need to carefully evaluate the mechanisms they already have in place or will need to put in place in order to accommodate this type of community involvement.

Members of the Police Foundation national advisory board strongly advise that agencies considering a sUAS program begin the process of community engagement very early on. Departments that were successful in creating a sUAS program said they made community outreach a central feature of their planning. Recommendations for building dialogue with the community and stakeholders include:

- **Outreach should be done early and often.** An outreach plan should be one of the first elements of any effort to create a sUAS program. Law enforcement executives should have their departments set forth all of the policies, procedures, and prohibitions that will be part of a sUAS operating plan. The plan should be presented to policymakers and community groups before a sUAS is purchased. Avoid letting the first mention of a "police drone" be a request to purchase, even with grant funds.

- **Create opportunities to gain input from the community**. Engaging the community and building dialogue with relevant stakeholders is ultimately a process of conscientious, concerted, and continual exchange, not a one-time presentation. There are many tangible steps that law enforcement agencies can take to ensure the community's voice is represented as well as to establish and maintain a solid foundation for these types of dialogue. These include the following:

- Surveys (both within the department, and of the community)

- Town hall meetings

- Citizen police academies

- Leveraging the media (interviews/talk shows)

- Roll call presentation/discussion (to engage and educate line officers)

- Focus/discussion groups (to engage departmental staff)

- Focus/discussion groups (of other government/public safety organizations, such as fire/EMS, etc.)

- Executive meetings (with the chief/mayor, other governmental leaders, community leaders)

- Public resources page (on the department website)

- Social media

- Citizen Advisory Board (could be convened to assist in conducting cost-benefit research; defining onboard equipment needs; and reviewing UAS policy)

- Incorporating community residents (particularly those with certifications in flight operations) into volunteer positions or programs.

- **Explain how you will protect privacy and maintain safety.** Accept that privacy and safety concerns will be a source of opposition, and confront them directly by ensuring understanding and incorporating strategies to address legitimate concerns into decisions regarding UAS policies and procedures. The community should be reassured that the department's sUAS will not be used to collect information that is not necessary for legitimate police use. If possible, meet in advance with privacy advocates and community groups to hear concerns and address them. Ensure that personnel speaking on behalf of the department on UAS issues are knowledgeable not only in departmental policy, but also in UAS law and regulation, model policies and best practices. If your agency has conducted a PIA or drafted a privacy policy, those actions should be described and shared as appropriate. Give serious consideration to the creation of a community advisory board that provides a mechanism for regular, consistent two-way communication regarding sUAS operations. The IACP technology policy framework, included as Appendix 16 of this guidebook as a resource for policy development, lists nine universal principles for policy development concerning the use

of "technologies [such as sUAS] that can or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data was captured" (IACP 2014).

- **Don't simply avoid the word drone, but define your aircraft.** Understand that even if the department avoids using the term drone, the public and media will insist on using that word for any unmanned aircraft. The best way to confront the negative connotation is to explain how the law enforcement UAS is different, and reinforce benefits to the community. Having your sUAS on display in meetings will help to convey what the technology really looks like all the while reinforcing that it is not a drone.

- **Emphasize public and officer safety benefits**. Every reference to UAS should emphasize benefits for the community. Search and rescue, officer safety at active shooting events, time and cost savings for accident and crime scene investigation are prime examples. Avoid calling the sUAS a "law enforcement tool." Make it clear that the sUAS will **not** be gathering "intelligence;" used for revenue generation; or used in any way as a weapon. Watch for chances to promote how the sUAS is benefiting the community, and solicit the community for their thoughts on how the new tool may be used to benefit community safety. Alert local media to success stories from other jurisdictions, when possible.

Language that can help garner community support for sUAS includes

  - The ability to search a large area for lost children or adults (particularly those with special needs) more quickly and at a fraction of the cost of sending searchers, dogs, or traditional aviation units.
  - The capability to quickly locate potential suspects in difficult terrain (Stone 2014) or in areas where officers might be subject to ambush (KPIX 2015) by an armed assailant.
  - Speedy and more accurate collision or crime scene reconstructions that can cut officer person-hours expended in half and reduce the time needed to redirect traffic.
  - Review of fire or flood damage without the need to subject police and fire personnel to dangerous conditions.
  - Disaster relief potential to locate victims and more quickly direct rescuers.

- **Lay out a legal game plan and explain it.** Ask the district attorney or your department's legal advisor to draw up a memo outlining the laws protecting privacy and how the sUAS program will adhere to them. Make it clear that in most non-emergency cases, a warrant will be secured before the sUAS is used. Focus on a detailed explanation of data collection, retention and use.

- **Work with fire agencies on disaster relief assistance.** Reach out to the fire department to develop ways the sUAS can be used in support of fire emergencies or prevention. Have fire officials attend community outreach events. Some Police Foundation focus group members suggested the fire department might take the lead on presentations to emphasize the public safety mission of the sUAS.

- **Keep the sUAS in the open and emphasize transparency.** Maintain the maximum possible transparency throughout the effort to acquire a sUAS. Invite the media to test flights when feasible, and make members of the team available for interviews. Ensure that everyone involved with the program emphasizes the benefits to the community and limits on use, as opposed to just how "cool" the technology is.

- **Maintain transparency once the sUAS is in operation.** Use traditional and social media to keep the public informed. Both the Mesa County Sheriff's Office (Mesa County Sheriff's Office 2015) and Arlington Police Department (Arlington Police Department 2015) make it easy to find information about their sUAS programs on their websites, and provide detailed "frequently asked questions" sections.

Agencies should continue to leverage existing tools used to engage stakeholders and community members on other law enforcement efforts, extending those tools to include UAS orientation. In addition, the COPS office offers resources on ways to foster consensus in a community, as well as guides on best practices for successfully establishing new technology in police departments.

Final determination of need

In a 2015 sUAS concepts and issues paper[14], the IACP recommends the needs assessment as the very first step an agency should take when considering the introduction of any new and emerging technology into a department. A final determination of need will require aggregation of findings from the technological, cost-benefit, and legal research conducted as well the community and stakeholder input obtained. In order for successful planning, implementation, training, deployment, use, and management of sUAS technology to subsequently take place, the final determination of need must have been made with thoughtful consideration of not only the technology itself but also the community and stakeholder sentiment regarding it.

Summary

It is important for agencies to conduct a methodical assessment of community and department needs, making thoughtful consideration prior to determining if UAS technology is right for their community. While decisions to acquire new technology should always be driven by organizational mission and demonstrated need, for police departments using community-policing philosophies, assessing the need for a sUAS must also start with a scan of community and stakeholder sentiment regarding the technology. Determining whether your community is ready for UAS technology is a critical component of a needs assessment. A final determination of need should aggregate the findings from the technology research, cost-benefit research, and legal research conducted along with the community and stakeholder input obtained.

14. Included in Appendix 15 of this report.

CHAPTER 11

Developing an Operating Plan

Once a needs assessment has been completed, if the community has been determined to be ready for UAS technology, law enforcement agencies should create an operating plan. The plan should detail

1. How the sUAS will be used in the community;
2. How safety will be maintained when operating the sUAS;
3. How the public's privacy will be protected.

These plans should be developed before actually purchasing a sUAS, and should be shared with the public and policy-makers to ensure the intended use of the sUAS is understood and supported. More importantly, development of an operating plan ensures that departmental personnel have thought through and are knowledgeable about these important issues as they move forward.

ADVICE FROM THE ADVISORY BOARD |
Law enforcement agencies should never move forward to purchase a UAS until they have developed the plans for how it will be used, how safety will be maintained, and how privacy will be protected. These plans must be shared with the community and policymakers, or the chances are good that the community will not support the decision.

Components of the plan

There are five fundamental areas that must be carefully planned before a law enforcement agency sets out to use a sUAS. It is vital that these plans be made in advance and provided to the public, media, and policymakers for review, input, and understanding.

1. **How will the sUAS be used?**
   Determine what the department is going to do with a sUAS, be specific, and draw up those protocols in writing. The plan should also include clear delineations on what the sUAS will NOT do.

2. **Explain the laws that govern UAS use.**
   Research and explain the laws and regulations that govern law enforcement use of UAS. Doing so will let the public know that you understand the limits of use. Include reference to constitutional protections, state legislation, municipal code, industry standards, open government laws, and departmental policy as they apply to UAS.

3. **Discuss who will be involved in operating the sUAS and how safety will be maintained.**
   Develop a working plan that details who will operate the sUAS and when; how they will be trained; what measures will be taken to ensure the safety of the operators and the public; and how adherence to the plan will be documented. The plan should outline in detail how the decision to deploy the sUAS will be made, who will make it, and what limits will be put on its use. More detailed information on staffing and training can be found in Chapter 13 of this guidebook.

4. **Clearly define what information the UAS will collect; how and when it will be collected, maintained and stored; and who will have access to the data.**
   Decide what data is going to be collected (photos, video, environmental monitoring). Define how the data will be used—for investigations, accident or crime-scene reconstruction, or even possible court cases. Set a time limit on how long the data will be held and determine who will have access to the data while it is maintained and how the data will be destroyed. Explore using a PIA (Bureau of Justice Assistance 2012), a privacy policy, and/or something similar to address privacy issues before they become a widespread community concern.[15]

15. An example of a PIA can be found in Appendix 10 of this report.

For example, the maintenance of extensive video and other surveillance technology files is a legal issue that has become increasingly troublesome for law enforcement. Citizens have used state and local open-records laws and groups to seek access to all files collected using such technologies as license plate readers (Farivar 2015) and police body cameras (Reporters Committee 2015). Advisory group members strongly suggested that police agencies research the potential effect their state laws might have on any retained video files from UAS and develop policies on how to deal with access requests before a sUAS program is in place.

5. **Engage the community in conversation regarding sUAS program planning, including addressing privacy and other concerns.**

   It is important that the community be aware that the issues above are being carefully addressed. Ensure that all information regarding UAS data collection is made available to community members in an easily accessible format and location, and that there are forums for the community to hear about project status and to communicate suggestions and concerns.

WHAT IS A PIA? | A Privacy Impact Assessment (PIA) is a decision making tool used to identify and mitigate privacy risks at the beginning and throughout the development life cycle of a program or system. It helps the public understand what information is being collected and how it will be used, shared, accessed and stored.

Recommended standards for UAS operations

The Association for Unmanned Vehicle Systems International, which represents the UAS industry, has developed a Code of Conduct (AUVSI 2016) that includes recommended standards for operating a UAS.

It calls on operators to ensure UAS flights will be conducted only after a thorough assessment of risks associated with the activity, including

- 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.

The Remote Control Aerial Platform Association also provides extensive guidelines (RCAPA 2016) for the safe operation of a UAS. These guidelines provide a strong foundation for law enforcement agencies, and should be consulted when developing UAS operating plans.

Summary

There are five fundamental areas that an operational plan for UAS use should address. At a minimum, an operating plan should address how the sUAS will be used in the community, the laws governing its use, procedures for ensuring operational safety and guidelines for protecting the public's privacy. The advisory board recommends that these plans be shared with the public, media and policymakers for review, input, and understanding.

The next section in this guidebook provides a roadmap for sUAS program planning.

IV – sUAS Program Planning

CHAPTER 12

Developing Departmental UAS Policy, Procedures, and Guidelines

As with implementation of any new technology, developing and vetting detailed UAS policy (i.e., operating guidelines, uniform policy, or standard operating procedures) well in advance of first use is critical. Departmental UAS policy should clearly define how departmental personnel are permitted to use UAS technology to increase public safety. In 2015, the IACP released a model policy for law enforcement agencies to use as a springboard for creating their own responsible use and deployment policies. The sUAS model policy can be found in Appendix 15 of this report.

FOCUS ON THE FIELD | Police agencies that have established successful sUAS programs report that citizens have been supportive of any use of sUAS as long as a warrant is obtained. Officials from agencies including the Arlington (Texas) Police Department and the Mesa County (Colorado) Sheriff's Office agree that any use of sUAS beyond that allowed in a warrant should be spelled out in departmental policy and must be approached through the lens of how it will benefit the public rather than as a law enforcement tool.

Taking this proactive approach before acquiring any type of sUAS equipment can help avoid legislative showdown; allay public fears of a "big brother state;" help shape legislation to preserve civil liberties; and allow police access to efficient and cost-effective public safety technology by ensuring its use complies with the Fourth Amendment. Where the community is not involved in these policy decisions, they are unlikely to buy into the sUAS program. For example, in the first community meeting held by the Seattle Police Department to explain to the community the intended use of two newly acquired 3.5 lb Draganflyer X6 Helicopter Techs, the Chief was drowned out by references to George Orwell's *1984* (Clarridge 2012).

ADVICE FROM THE ADVISORY BOARD | The public is more likely to support a new police technology if they understand how it will be deployed. Draft solid guidelines and policies, and communicate them with your community.

Checklist for developing UAS policy and procedures

While departmental UAS policy, procedures, and guidelines differ between law enforcement agencies based on specific community and department characteristics, there are a number of common steps to take to ensure solid policy development. Those steps are:

- **Conduct constitutional/legal research and/or consult legal counsel.** It is critically important to address the legal implications of UAS in departmental policy. A strong legal foundation, along with an understanding of community concerns about privacy and safety, should be the blueprint for permitted use of UAS. In addition, many state laws and regulations will impact how departmental policy is written. For example, some states require that the UAS have an airtime recorder, and that only the supervising officer have access to be able to reset the timer. State protocols such as those in Virginia (Virginia Dept. of Criminal Justice Services 2013) are typical in that they require the supervising officer submit a quarterly update of flight logs, which are made available for public inspection. Virginia's protocols call for a disciplinary procedure to be established for any unauthorized use of the UAS. While Section II of this guidebook provides a summary of legal and regulatory considerations for UAS use, and a high-level review of legal memoranda can be found in Appendices 10a-f, a knowledgeable legal

consultant can provide a more detailed analysis of laws that impact your community.

- **Understand industry guidelines, models, and standards that apply.** The International Association of Chiefs of Police (IACP) Aviation Committee's *Recommended Guidelines for Use of Unmanned Aircraft* should be the starting point for any law enforcement agency endeavoring to create departmental policy for a sUAS program. The guidelines should act as the foundation from which to build more detailed policy. The IACP sUAS model policy is included in Appendix 15 of this report. Also, consult the FAA's webpage, Unmanned Aircraft Systems (faa.gov/uas).

- **Reference departmental UAS policy from agencies that have established functioning sUAS programs.** Contact agencies with established sUAS programs to share information on policies that have been successful in their community, and ones that have caused problems.

- **Provide detail on procedures.** Detail specific UAS procedures for departmental personnel. This may include the operational system, training, data retention, and community engagement procedures, among others. For example, departmental policy and procedures should define when a sUAS would be used to support the execution of a warrant, and what activities might be undertaken when a warrant is not involved. Review how a sUAS could provide support capabilities in situations where the department will already be seeking a warrant. Other examples include defining data retention policies, and detailing how deployment decisions will be made (chain of command, etc.).

- **Draft a "facts and circumstances" checklist.** A reviewing court will look closely at the facts and circumstances of a particular situation when assessing the legality of police use of UAS to monitor, search, and gather electronic data. Consider beforehand the facts and circumstances that a reviewing court will look at in making a determination about the constitutionality of the UAS usage in question, and create a checklist to capture that data. At a minimum, the checklist should include the location of the search, the specified purpose of the search, a description of the technologies used in the search, and the type of data that was captured (e.g., communications, GPS tracking, video or thermal imaging data, etc.), an assessment of how sophisticated the technology used is, and an evaluation of the current understanding of privacy in your community and how it would apply to the facts of the case in question (McKenna 2014b).

- **Put all information together into a policy packet, and make it easily accessible to department personnel, stakeholders, and the public.** Strong community policing is predicated on transparency and the engagement of community members. Developing strong UAS policy is a critical juncture in designing a sUAS program, and should include involvement of stakeholders and members of the community. Make UAS policy available for review and comment by community members and other stakeholders prior to deployment of the sUAS, as well as throughout the life of the program.

- **Regularly review, evaluate, and update UAS policy.** Departmental policy should be updated on a regular schedule to ensure accuracy and avoid obsolescence. New policy should receive more frequent attention as it is used and shaped, and the public should be informed of substantive changes in UAS use or policy.

Prohibitions

Many focus group and advisory board members urged agencies to specifically and publicly prohibit certain UAS capabilities in order to foster public trust. Some activities that should be flagged as prohibited by departmental policy include the following:

- **Any use of force involving a UAS, including weaponization.** Media reports have speculated on whether domestic UAS could be weaponized. The IACP, in its Recommended Guidelines for the Use of Unmanned Aircraft (IACP 2012), has "strongly discouraged" equipping law enforcement

sUAS with weapons of any sort and its sUAS Model Policy states, "(t)he sUAS shall not be equipped with weapons of any kind." Further, it is recommended that the agency have the sUAS manufacturer certify that the air vehicle, as delivered, is not capable of carrying, or deploying, weapons of any kind.

- **Generalized patrol and intelligence-gathering missions.** Focus group members suggested that garnering public support for a sUAS that will be used in general intelligence-gathering activities would be extremely difficult. Such use of sUAS may also violate the First and Fourth Amendments.
- **Data-driven information gathering, such as crowd monitoring or estimating during peaceful demonstrations; or revenue-generating such as monitoring traffic or parking areas.** Reports of the ability of sUAS-based cameras to provide images for facial recognition software or license-plate readers have been leading causes of public antagonism against law enforcement sUAS.

U.S. Department of Justice guidelines for Federal law enforcement use of UAS

On May 22, 2015, the U.S. Department of Justice released guidelines (DOJ 2015) for the use of UAS by all federal agencies. The guidelines, which can be found in Appendix 14 of this report, were developed by a task force of representatives from most federal agencies that may make use of UAS for domestic purposes. The guidelines call on federal agencies to adhere to the following protocols in UAS use:

- Operational consistency with the U.S. Constitution, especially the First and Fourth Amendments.
- That the UAS never be used solely to monitor activities protected by the First Amendment, or in any way that runs counter to the department's policies protecting against discrimination based on race, religion, gender, sexual orientation and national orientation.
- That federal agencies weigh the potential for UAS operations to intrude on citizens' privacy and, whenever possible, select a less intrusive practice.
- That the UAS be used only in operations authorized by a senior official. A warrant will be required in any investigation that would require a warrant under current practices.
- That any video footage or other data gathered in an authorized investigation only be retained for 180 days or until completion of the investigation.
- That each agency conduct an annual review and report on all activities involving unmanned aircraft systems. A website can aid in providing access to information that is not involved in an ongoing investigation.

Summary

While there is no model policy that can meet all the needs of every law enforcement agency, in this chapter we have attempted to present a number of important steps that can be taken in order to ensure solid policy development for a law enforcement department's use of sUAS. Among the sources of guidance currently available to law enforcement agencies are the 2015 U.S. Department of Justice guidelines for the use of unmanned aircraft systems; the IACP Aviation Committee's *Recommended Guidelines for Use of Unmanned Aircraft*, along with their 2015 model policy for sUAS; existing state protocols; and departmental standard operating procedures from law enforcement agencies with existing sUAS programs. For example, the Mesa County (Colorado) Sheriff's Office and Arlington (Texas) Police Department standard operating procedures can be found as appendices to this guidebook.

The next chapter discusses key aspects of training and staffing a sUAS team.

CHAPTER 13

Staffing and Training the sUAS Team

High standards for sUAS crew professionalism and training demonstrate agency commitment to public safety and support. Reports of irresponsible use of sUAS (usually by private citizens) have left many in the community concerned that sUAS use can be hazardous to public safety. Law enforcement agencies that have established successful sUAS programs suggest maintaining transparency about high safety standards; time devoted to training; and level of safety accountability assigned to each member of the team. When a sUAS crew is experienced in manned aviation, the department should further ensure that the community is aware of the sUAS crew's background and experience as members of the department's aviation unit.

Staffing

In Part 107, the required minimum flight crew consists only of a Remote Pilot in Command (RPIC) for civil operations. Other crew members may include a visual observer and a person who manipulates the controls of the sUAS, under the direct supervision of the RPIC. For public aircraft operations, the COA establishes the minimum flight crew.

Assigning these additional personnel to the sUAS operation helps a sUAS team comply with the requirement to be able to see the aircraft through the entire flight. The FAA recognizes that the person maintaining visual line of sight (VLOS) of the aircraft may unavoidably lose sight of it for brief moments, either because the aircraft momentarily travels behind an obstruction or to allow the person maintaining VLOS to perform actions such as scanning the airspace or briefly looking down at the sUAS control station. However, FAA rules emphasizes that even though the RPIC may briefly lose sight of the aircraft, he or she is still responsible for the see-and-avoid provisions set out in FAR Part 107 or COA.

The supervisor of the sUAS team and the RPIC should confer during preflight planning to determine the minimum number of personnel required to safely and effectively conduct the flight. All members of the flight crew must maintain effective communication with each other at all times.

FOCUS ON THE FIELD | While only one UAS crew member is required by the FAA, many law enforcement agencies have added additional crew to increase operational capacity and safety. Both the Arlington (Texas) Police Department and Mesa County (Colorado) Sheriff's Office have at least three sUAS crew members on their respective teams.

While only one UAS crew member (the RPIC) is required by the FAA, many law enforcement agencies have added additional crew to increase operational capacity and safety. Standard operating procedures for Arlington, TX Police Department list a Special Operations Commander, Team Leader, Assistant Team Leader, Pilot in Command, Observer, and Camera and Remote Sensing Operator as integral personnel in a sUAS team, all with clearly defined roles. Mesa County Sheriff's Office standard operating procedures list a commanding officer, supervisor, and operator(s) among the required personnel.

While the specific number of personnel comprising a sUAS team will undoubtedly vary in number, law enforcement agencies successful in creating a UAS operation have included a video or image operator (sometimes referred to as a sensor operator) to control the camera or infrared image independent of the pilot if necessary, and to monitor images produced in the search or investigative operation that is underway. Further, both the Arlington Police Department and Mesa County Sheriff's Office have added a more senior officer who serves as the decision-maker for operations and as the communications liaison with other law enforcement units; this officer

also coordinates with local air traffic control to request permission for the operations, as required by FAA rules. In Mesa, the RPIC has final fly/no fly decision-making authority. In these cases, the inclusion of additional personnel is aimed at ensuring safe operation and minimizing risk to people, property, and aircraft.

In both Arlington and Mesa, sUAS crews have been drawn from officers who are already members of the force. In many agencies, sUAS pilots are well-trained and responsible members of their department's manned law enforcement aviation units. Law enforcement agencies that have completed an operational COA have devoted only a portion of staff time to sUAS training and operations, and are able to retain other duties. Even during the initial certification process, while the designated sUAS team lead spent time working with the FAA to refine and complete COA requirements, his or her hours were only partially spent on those tasks. As of the end of 2015, Mesa has amassed over 300 flight hours across 85 missions, with an average flight time of 20 minutes. In total, they report that they have assembled and flown their sUAS an average of 900 times (Benjamin Miller, personal communication).

Chain of command

Agencies that have existing sUAS programs have defined a clear chain of command outlining who will decide when the sUAS is to be used; what measures will be taken to protect the safety of the operators and the public; and how adherence to the plan will be communicated to the public and media. These requirements are routinely documented in the department's sUAS operating plans, as well as departmental policies and procedures documents.

FOCUS ON THE FIELD | Mesa County (Colorado) Sheriff's Office requires that the request to fly a sUAS be made by a sergeant or higher-level executive. The officer in charge of the unit is a specialist in sUAS use with flight training.

Police Foundation Advisory Board members suggest that command level officials have the responsibility to control sUAS deployment, and that the request to deploy should come from a sergeant or higher rank. They suggest that the pilot or operator should decide when it is safe to fly and under what conditions, and when to abort the flight due to safety issues.

Training

Training for a sUAS pilot's license takes up to 40 hours (Aircraft Owners and Pilots Ass'n. 2015) and can cost between $5,000 and $9,000. Professional training for a certificate in flying unmanned aircraft systems (Unmanned Vehicle University 2015) can take 30–40 hours and cost $3,500. However, most manufacturers provide training (Draganfly 2015a) in flying and maintaining their aircraft that limits the time to just days, and the cost to around $500–$1,000.

While not required by Part 107, law enforcement agencies are encouraged to fly in a designated remote area until the sUAS team achieves proficiency in flight operations. The sUAS team also needs to fly the system with sufficient frequency to maintain proficiency. Additional training may be required for video and sensor operators to maintain their proficiency.

Summary

Federal Aviation Regulations (FAR), Part 107 only requires one sUAS crewmember—a Remote Pilot in Command (RPIC). The use of additional team members is encouraged to ensure that the aircraft remains within sight, avoids obstacles or other aircraft while in operation, and is able to conduct the mission efficiently and effectively. Part 107 also establishes RPIC licensing requirements, as well as other limitations imposed on a particular operational activity involving a sUAS. Police Foundation Advisory Board members suggest that command level officials have the responsibility to control sUAS deployment, and that the request to deploy should come from a sergeant or higher rank. High standards for sUAS crew professionalism and training demonstrate agency commitment to public safety and support.

CHAPTER 14

Leveraging the Media to Communicate with the Community

A scan of national news stories focused on sUAS, reveals that most media outlets and much of the public are predisposed to react with skepticism, or even downright hostility, to the idea of sUAS in their community. There is no question that some law enforcement agencies have faced swift and noisy opposition to their acquisition of a sUAS. Polls consistently show that a third or more of people strongly fear losing their privacy (AP 2012) if sUAS are used in law enforcement activities. But many of the same polls reveal that 80 percent or more of Americans support using sUAS for search and rescue (Monmouth University 2012).

Community policing advocates recommend police partnerships with the media as a beneficial strategy for helping to raise public awareness and encourage participation in community-based projects. While it may not be immediately obvious, a police-media partnership can quickly become a powerful mechanism through which police agencies can both deliver the UAS public safety message, and also gain insight into community concerns regarding their use. Upon being granted a COA for a sUAS, the Grand Forks County Sheriff's Department sent out a press release to the media and community, describing the sUAS and detailing the jurisdiction and restriction on use. Proactively informing the media (and community) in these types of situations can go a long way in mediating initial reactions to unexpectedly encountering a sUAS on a morning walk, for example.

FOCUS ON THE FIELD | Upon being granted a COA for a Draganflyer X6 sUAS, the Grand Forks County Sheriff's Department sent out a press release to the media (and community) describing the sUAS and detailing the jurisdiction and restrictions on use.

In addition, a media partnership can also help law enforcement develop more comprehensive media strategies, such as sponsoring crime prevention initiatives and helping to design public education campaigns around a particular public safety issue. In jurisdictions where prior experiences with the media have been negative, these partnerships may not seem like a good idea, but they have benefits if approached proactively with trusted media partners. In situations where relationships with the media are strained, partnerships with specific community members, community service providers, or groups of volunteers, activists, or community leaders can be engaged in achieving specific goals. The community-oriented policing philosophy recognizes that community-based organizations that provide services to the community and advocate on its behalf can be particularly powerful partners (COPS Office 2014).

To provide insight into how the media could help spread an agency's UAS message, here are some examples, both recent and long-standing, of positive and successful police-media partnerships in other public safety areas:

- **Cleveland, OH.** The mayor enlisted the help of a local television station and radio station to announce the city's gun exchange, violence reduction, and crime prevention initiatives. In addition to helping announce the initiatives, the stations also operated phone banks for donations (Nat'l Crime Prevention Council 2015). This partnership, launched in 1994, still continues today (Pollack 2014).
- **Oakland, CA.** In 2014, the Oakland Police Department announced a new partnership with the social media company Nextdoor to craft a professional and consistent social media presence. Chief Sean Whent told the *San Jose Mercury News* on April 25, "open and direct communication with the community

has a lot of value for us." The partnership had the full support of Oakland Mayor Jean Quan, and members of neighborhood groups.

- **Amber Plan.** Created in 1996, the Amber Plan is a voluntary partnership between law enforcement and broadcasters to inform the public that a child is missing. The DC AMBER Task Force includes the Child Exploitation Subcommittee of the Metropolitan Washington Council of Governments Police Chiefs Committee, local broadcasters, key leaders in the community, the National Center for Missing and Exploited Children, and numerous radio and television stations that have committed to participate (District DOT 2005).

- **CrimeStoppers.** The CrimeStoppers television segments are an example of the longstanding success of a collaborative partnership between the police and the media to inform the public about ongoing investigations on which the public can provide information (Crime Stoppers USA 2015).

Law enforcement agencies that have been active in promoting community policing recognize the value of reaching out to citizens, policy-makers, and the media in developing the plan to create a sUAS unit. There are a few key components that an agency interested in developing media specific to sUAS should consider:

- Emphasize potential benefits to public/community and officer safety, the limits on uses, and how privacy and liability concerns will be addressed.

- Make it a point to use the media in sharing success stories of how the sUAS is benefiting the community. Alerting the media to success stories from other jurisdictions may also be helpful. Quickly publicizing any discovered misuse and the disciplinary response will also demonstrate that oversight mechanisms are working.

- Maintain transparency at all times. This is where the DoD policy of *maximum disclosure, minimum delay* to inform the American public may serve as a useful guide. If information cannot be released because of operational concerns, be clear about that. If there is a timetable for the release of information, make sure that timetable is accurate and is communicated accurately. Transparency can be emphasized by inviting the members of the media to test flights whenever feasible. Making members of the team available for interviews and questions can go a long way toward clearing up misconceptions and satisfying curiosities.

Traditional media & UAS

Media strategies should make use of a wide variety of platforms, including local television, the Internet, radio, and newspapers. For example, a local television station could air a demo of the UAS; a radio station could produce a discussion on the uses and challenges of UAS in the community; and a newspaper could run a story on the program's first major success. In 2013, the Arlington (Texas) Police Department's aviation unit and public information department created both an aviation equipment demonstration video and information video on the Avenger UAS. The Mesa County Sheriff's Office has leveraged the media to discuss both successes and failures in their use of sUAS. Ben Miller, former UAS program director for the Mesa County (Colorado) Sheriff's Office, has spoken candidly about successes as well as two search and rescue operations in which the county's UAS were unsuccessful (Greene 2013). Additionally, both the Mesa County Sheriff's Office and Arlington Police Department make it easy to find information about their sUAS programs on their respective websites, and provide detailed "frequently asked question" sections.

Social media & UAS

Social media offers opportunities to connect and partner with segments of the community that may not be reached as readily with traditional media. In a recent survey, the Police Executive Research Forum (PERF) found that police are increasingly open to embracing a variety of social media platforms, a trend that is expected to continue to grow in the next several years (PERF 2014). Many departments have successfully employed social media to disseminate information to the public. Many community groups have newsletters and Facebook pages that they regularly update, which offer excellent platforms for law enforcement to

communicate. Social media also provides an organic means through which to receive input and comment from followers in the community.

Similar to individual and community partnerships, each partnership with local media outlets will be unique. Because of this, there is no standard media plan that will be relevant to all. What we have presented here are strategies that have worked for Mesa County, Arlington, and a number of other cities and jurisdictions. The keys for a law enforcement agency in developing a media partnership strategy are proactive engagement, unwavering transparency, and a multipronged approach for getting department-crafted messages about sUAS to the public.

Summary

Community policing advocates recommend police partnerships with the media as a beneficial strategy for raising public awareness and encouraging participation in community-based projects. Law enforcement agencies that have been active in promoting community policing recognize the value of reaching out to citizens, policy-makers, and the media in developing the plan to create a sUAS unit. Similar to individual and community partnerships, each partnership with local media outlets will be unique.

V – Program Implementation

CHAPTER 15

Program Implementation and Evaluation

Program implementation

Because so few law enforcement agencies have implemented an operational sUAS program, the steps to full implementation are less defined than are the planning steps. Prior to becoming operational, the law enforcement agency should conduct extensive training to assure proficiency in all phases of sUAS operations. During this training period, the sUAS crew can develop its own expertise and practice simulated missions with other agency teams (Search and Rescue, SRT, Emergency Management, CIS, etc.), in order to establish the processes and protocols that will ensure safe operations and the satisfaction of mission requirements. This training and on-site evaluation period can last a few months or a year or more, depending on the effort the agency devotes to training and the different types of mission scenarios the sUAS team is learning to support.

Despite the paucity of existing guidance on the proper implementation of UAS technology, considered a new and emerging technology for public safety use, significant guidance can also be drawn from the implementation of other technologies such as dash cams, radios, and thermal imaging. In all cases, the implementation of appropriate technology by law enforcement agencies should be designed with consideration for local needs and in alignment with national standards.

Focus on the Field | The Mesa County (Colorado) Sheriff's Office, whose territory is primarily rural or open space, completed the onsite training stage in *approximately six months*. The Arlington (Texas) Police Department, whose jurisdiction includes urban areas and the Dallas-Fort Worth International Airport, *required more than a year* to gain FAA certification to achieve operational proficiency.

Community engagement during implementation

While the time required for full operational status may vary, it is important to continue the effort to engage the community, maintain a community policing focus and provide a high level of transparency, particularly during the initial steps of implementation. Agencies with existing UAS operations say that many people's attention begins to focus on the new sUAS program when the aircraft are in the air. Making community engagement a priority throughout the program's development and implementation reduces the risk of rumor and false information and increases the community's sense of ownership in both the new program and the coproduction of public safety.

Recommended community engagement steps during implementation include the following:

- Seek out opportunities to educate the community about the sUAS program, and to be educated by the community about their concerns and suggestions.
- Invite the media and community leaders in small groups to a training mission where the sUAS are being utilized to demonstrate how the sUAS team works to protect safety and privacy.[16]
- Work with existing stakeholder organizations such as citizen advisory boards to involve members of the community and to gain their perspective.

16. Flights strictly for the purpose of demonstrating the capabilities of the sUAS, for the media or community, would fall outside the authorized uses of a public aircraft operation (if the agency is operating the system as one). However, the media or members of the community may observe authorized training flights conducted by members of the sUAS team. The agency must assure they remain clear of the area where the sUAS is being flown.

- Work with the media to inform the community of scheduled testing being led by the department and leverage them to discuss both successes and failures in the department's use of UAS.
- Make it easy to find information about the sUAS program on the department website and provide detailed answers to frequently asked questions.
- Post photos and video on the agency website and provide links and updates on the agency's social media platforms.
- Send the sUAS team to community group meetings to display the sUAS and explain the agency's plan of operations and the commitment to safety and privacy.
- Maintain an open-door policy for community members who call with concerns or criticisms regarding the UAS operation. The Mesa County Sheriff's Office invites every citizen who calls to come see the sUAS and discuss their concerns in person.

Agencies with successful sUAS programs operate with a policy of high-level transparency and community outreach, which continues once full operational status is realized. They publicize successes and take a community policing approach that allows the community to take ownership of the sUAS and understand its public benefits. Even when a search operation does not result in finding the missing person, publicizing the benefits (Fox Business 2014) of using the sUAS can bring positive media and community support.

UAS operations

Implementation of UAS operations should follow the steps outlined in operating plans and policies developed during the planning phase. The sUAS crew and staff should understand and comply with their duties and roles once the program is implemented. The sUAS crew will likely be able to undertake UAS tasks while continuing with other duties; however, in addition to the official operations, agencies require an average of 16 hours of training per month to maintain standards. The FAA requires aeronautical knowledge currency for civil RPIC certificate holders. It does not require operational currency; however, agency executives must nonetheless ensure that sUAS team members maintain operational currency on the system. Additionally, many municipalities and state governments have established legal requirements for reporting of law enforcement UAS operations. The completion and presentation of these reports provide another outlet for community engagement through publicity and transparency.

Program evaluation

Once implementation of the sUAS program has occurred, it is important to engage the community in the evaluation process. This process should be designed to allow law enforcement executives and program staff to evaluate and report on the impact of a sUAS program so that any necessary adjustments may be made, and should include both qualitative and quantitative evaluation. Community input through strategies such as surveys, social media comment solicitations, and town hall meetings will likely provide qualitative comments reflecting the community's perception of the program. In addition, department personnel can provide perspective on their interaction with the sUAS, whether it helped them resolve a call or a case, and ways the program could be more useful to them. Quantitative data should be collected by sUAS program staff, and reported regularly. A locally appointed board with privacy credentials can establish metrics for assessing performance of the program. Data that should be collected may include basic information such as mission date, time, purpose, staff, and outcome.

Both the Mesa County Sheriff's Office and the Arlington Police Department perform evaluations of various aspects of their sUAS programs in order to revise their operating plans to ensure the highest level of efficiency and effectiveness. These evaluations, detailed in the SOPs included as Appendices 12 and 13, include reviews of data maintenance and related policies, equipment, training, and personnel. It is important to inform the public of any substantive changes to policy or practice to ensure continuing public support.

The issues of UAS legality, safety, and technology are just now beginning to be explored, largely because of the scarcity of data available. Data on law enforcement responses to incidents involving their own sUAS is currently not uniformly collected. As the law enforcement community increasingly employs sUAS, decisions regarding regulation, training, technology and policy will need to be informed by sound data and research. In 2014, the Police Foundation was awarded a grant to develop a data collection and analysis platform, the National Public Safety sUAS Flight Operations and Incident Reporting System, which will be the foundation from which to identify the safest, most ethical, and most efficient ways to integrate sUAS into law enforcement operations.

Summary

Implementation of UAS operations should follow the steps outlined in operating plans and policies developed during the planning phase. Despite the lack of existing guidance on the proper implementation of UAS technology, considered a new and emerging technology for public safety use, significant guidance can be drawn from the implementation of other technologies such as dash cams, radios, and thermal imaging, to name a few. In all cases, the implementation of appropriate technology by law enforcement agencies should be designed with consideration for local needs and in alignment with national standards.

While the time required to achieve full operational status may vary, it is important to continue the effort to engage the community. it is important to continue the effort to engage the community, maintain a community policing focus, and provide a high level of transparency, particularly during the initial steps of implementation. Once the sUAS program is implemented, it is important to engage the community in the evaluation process.

CHAPTER 16

Ongoing Community Engagement

Continual community engagement throughout the life of the sUAS program requires strong collaborative partnerships between law enforcement agencies, individuals, and organizations in the community. It is important for these partnerships to be centered on developing long-term solutions and increasing trust. When selecting potential partners, it is vital to consider the public safety issues that are most prevalent in the community. This will help to identify the community members and groups, government agencies, nonprofit organizations, businesses, and media partners willing to be engaged in the program. True community policing requires collaborative efforts and commitment, by both police and community, to work toward a shared definition of public safety (Fisher-Steward 2007).

FOCUS ON THE FIELD | Here are some snapshots of the Arlington (Texas) Police Department (APD) community engagement strategy:

- **In early testing phases, APD worked with the media to inform the community of scheduled testing.**
- **APD made the rounds to every possible community group, showcasing the small UAS the department planned to use and laying out in detail how it would be used for community and officer safety.**
- **These show-and-tell sessions directly confronted concerns and laid out the department's policies for ensuring privacy would be protected.**
- **The APD's aviation unit and public information department created an aviation equipment demonstration video and information video on the Avenger UAS, respectively.**
- **APD makes it easy to find information about the UAS program on their website and provides detailed answers to frequently asked questions.**

Establishing community involvement with the sUAS program will be an ongoing process throughout the life of the sUAS program. It will mean continual solicitation, evaluation, and response to community input. Your agency may already have a sense of the concerns the community may have about sUAS; however, continual engagement of community partners will confirm or refine this information. Even if your agency's read of community concerns is spot-on, giving the opportunity to voice those concerns is an important and tangible step in engendering and cultivating trust.

Police Foundation focus groups provided the following recommended steps to continual development and maintenance of trust around UAS:

- **Language:** Carefully consider the language that will be used in constructing the UAS narrative the department will present to community stakeholders. "The introduction to the public is critical; you mess up that first step and you're going to be hard pressed to recover," said one focus group member.
- **Communication**: The majority of focus group participants believe that the biggest community concern police will come across is the violation of privacy and Fourth Amendment rights; therefore, it is important that all UAS policies be transparent and that police personnel be knowledgeable and able to communicate their knowledge about the legal aspects surrounding UAS.
- **Preparation:** Closely tied with communication is program preparation. Anticipate opposition or concerns throughout the process, and be proactive and prepared to address it. Whenever possible, address community questions and concerns before they come up. For example, one focus group member recommended utilizing reverse 911 technology to notify community members when sUAS flights were planned in an effort to allay fears or concerns when the public notices the sUAS flying.

- **Transparency:** What's going to be collected? How long is the information gathered going to be retained? Who can see it? What will it be used for? These are the questions that community members will want answered by the police in order to trust that law enforcement is being transparent about its use of sUAS in the community.

- **Impact:** Document information on deployments, successes, failures and why. Collecting this information will allow a department to provide information on community impact, whether good or bad. Documenting and highlighting successes centered on public safety to the communities will go a long way in changing opinion to the point that the public would consider it irresponsible not to use a sUAS in certain situations.

FOCUS ON THE FIELD | Here are some snapshots of the Mesa County (Colorado) Sheriff's Office (MCSO) community engagement strategy:

» **MCSO has leveraged the media to discuss both successes and failures in their department's use of sUAS.**

» **MCSO has for several years introduced their sUAS to the community at the annual Mesa County Safety Fair, where the sUAS team is available to showcase the aircraft, answer questions, and provide the opportunity for members of the community to see the systems up close.**

» **MCSO believes in maintaining an open-door policy for community members who call with concerns or criticisms of the UAS operation and invites every citizen who calls to come see the sUAS and discuss their concerns in person.**

» **MCSO makes it easy to find information about the sUAS program on their website and provide detailed answers to frequently asked questions.**

As part of an ongoing community engagement strategy, law enforcement agencies should seek ongoing feedback. Citizen satisfaction surveys, for example, are a great tool for departments to obtain input from the community, input which can be used to inform existing outreach and engagement strategies. Outreach also does not have to be confined to a department's jurisdiction. There are a number of agencies such as MCSO and APD that have successfully established UAS programs. These agencies can provide useful guidance on a number of issues related to sUAS acquisition and program implementation, including issues of community engagement and consensus.

Summary

Continual community engagement requires the formation of strong collaborative partnerships between law enforcement agencies, individuals, and organizations in the community. It is important for these partnerships to be centered on developing solutions and increasing trust. Establishing community involvement with the sUAS program will be an ongoing process throughout the life of the sUAS program. Police Foundation focus groups provided recommendations centered on language, communication, preparation, transparency, and impact for continual development and maintenance of trust around sUAS.

VI – Conclusion

UAS use in the U.S. is still in its early stages. With a regulatory framework now in place to enable regular, though limited, access to the NAS, uses of unmanned aircraft technology will be developed and refined. Development is expected to bring more powerful cameras and video, increasingly varied sensors, lighter and longer-lived batteries, and stronger basic materials and motors. The cost of a UAS, which has already dropped significantly in the past few years, is expected to decrease as more are produced and more companies compete for the business.

New capabilities and increased potential uses for UAS will almost certainly provide more value for law enforcement agencies. Even in the early stages, sUAS can be a force multiplier for public safety operations. One sUAS team can perform a search and rescue operation in a fraction of the time it would take ground teams, and with a team of four rather than dozens or hundreds. However, due to the novelty and fast evolution of the technology, the courts and federal regulatory agencies have struggled to catch up. Police are finding themselves having to work with limited constitutional guidance on the legal requirements for UAS. Law enforcement leaders see a valuable and relatively inexpensive tool in sUAS, with an unlimited potential for future use at a low cost, and finding ways to integrate a core public engagement element into a sUAS program in order to ensure success is proving to be paramount.

Indeed, privacy and civil rights concerns can overshadow any potential benefits in the minds of community members and stakeholders. The main challenges states and law enforcement will face will have little to do with technological capabilities and much to do with complex issues surrounding the collection of data (NASCIO 2015). Polls have consistently shown that a large majority of Americans are fearful that UAS will be used to spy in the United States, and they are adamantly opposed to that practice. Responding to that concern, President Obama has issued a series of orders (Executive Office of the President 2015) to federal agencies limiting the use of sUAS to specific operations, enjoining strict record-keeping, and limiting data collection, in order to encourage transparency in providing the public with information on when, why and how UAS are being used by federal agencies. The President also recognized that while UAS have the potential to be a transformative or "disruptive" technology in American society, the privacy, safety, and civil rights of citizens must be protected. He ordered the creation of a "multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues" as more UAS take to the skies.

The police profession must be able to convey to the community the benefits of sUAS for public safety while making it clear that civil liberties can be protected in every major scenario. They must also be able to convey the risks involved and the processes in place to mitigate those risks. This guide has attempted to address some of the most important issues across technological factors (safety; visual surveillance capabilities), legal issues (Fourth Amendment requirements; warrant requirements), operational considerations (pilot training and certification), community apprehensions (privacy; unauthorized dissemination; records retention), as well as ways to involve the community in conversation to further examine these issues.

Law enforcement agencies face renewed challenges in gaining and maintaining the trust of the communities they serve. In this environment, community policing principles of outreach, transparency, and public engagement are the most important tools available when attempting to start a new program that faces public skepticism. Agencies that have created a successful sUAS program have focused on outreach, transparency, and engagement first and foremost, letting the community know how this new technology can be leveraged in the coproduction of public safety and officer protection, enhancing community trust along the way.

Notes on Research Methods

Because unmanned aircraft systems are considered a new and emerging technology for public safety use, we found ourselves struggling to answer a myriad of issues and questions that have yet to be fully considered by law enforcement, the courts, researchers, and the public. In an effort to provide a preliminary yet comprehensive examination of some of the most pressing issues in the use of UAS for public safety purposes, the research and data collection approaches taken to inform this guidebook are primarily qualitative and content oriented. The research methods adopted to inform this guidebook consisted of the following:

- **Regional focus groups**
  Five local community-oriented focus groups were convened to discuss how UAS can help with policing operations, ways in which community members would like to be engaged by police to discuss UAS policy, and how to achieve consensus building, among other topics. Selected sites had to meet certain criteria agreed upon by both the Police Foundation and the COPS office. One of these criteria was that each police chief had to invite a representative of a community organization that had previously engaged their department on community policing issues to the focus group meeting.

- **National advisory board**
  The advisory board consists of a diverse group of specialists in the technological, regulatory, enforcement, legal, and privacy/civil liberties aspects of unmanned aircraft systems. They reviewed, discussed, and prioritized topics for inclusion into the guidebook, reviewed the guidebook outline and draft, and submitted comments and suggestions for improvement.

- **Case studies**
  In addition to participating in the National Advisory Board, the Arlington (Texas) Police Department and Mesa County (Colorado) Sheriff's Office, two departments that have successfully established sUAS programs with the full support of their communities, also provided us with extensive access to their policies, protocols and procedures, as well as expertise, to help ensure the accuracy of this guidebook.

- **Cost-benefit research**
  Areas of inquiry in the cost-benefit research included a scan of costs and benefits of using UAS for public safety and crime control objectives; a cost comparison between manned and unmanned aviation; and, to the greatest extent possible, a breakdown of costs and benefits according to function and application.

- **Legal research**
  The legal memoranda included in this report are the compilation of extensive research and analysis of the existing knowledge on the legalities and liability issues of using UAS for state and local policing. It includes an analysis of the variations in state and local jurisprudence as well as a review of Fourth Amendment jurisprudence.

- **Media research**
  Given the rapid pace at which this technology is being considered in the public safety arena, many of the most important issues related to its use are being addressed first and foremost in the media. As such, a scan of a variety of media sources such as news reports and blogs were deemed necessary. In our scan, we found that much could be learned from the successes and failures of departments that had attempted to acquire a sUAS, and more often than not, the media were the first to report on these successes and failures.

As sUAS slowly become a part of police department fleets across the country, future research directions are likely to include additional case studies and surveys of departments that have engaged in implementation attempts.

APPENDIX 1

UAS Cost-Effectiveness Issues

Table 3. Public safety and crime control functions of UAS

	Public safety	Crime control
Community Policing Functions	▪ Search and Rescue ▪ HazMat Response ▪ Disaster Response ▪ Traffic control	▪ Hostage Standoff ▪ Fugitive Apprehension ▪ Crime Scene Reconstruction
Cost/Quantitative Criteria	▪ Operating costs ▪ Cost per incident ▪ Pilot Training, Certification/ Recertification Cost ▪ Out year maintenance: UAS ▪ Out year maintenance: onboard equipment ▪ Liability insurance	▪ Operating costs ▪ Cost per incident ▪ Pilot Training, Certification/Recertification Cost ▪ Out year maintenance: UAS ▪ Out year maintenance: onboard equipment ▪ Liability insurance
Quantitative Effectiveness	▪ Operating time to locate/mitigate ▪ Rates of false positives/false negatives ▪ Onboard gear provides aids in clarity/accuracy	▪ Lower risk of ID error ▪ Assess area/victim/perpetrator conditions ▪ Aerial views reduce scene contamination
Qualitative Effectiveness	▪ Lives saved ▪ Increase in populations served ▪ Disaster response shortened ▪ Reduction of critical incident errors ▪ No air crews endangered ▪ Emergency management ▪ “Ground truth” available across policing	▪ More accurate subject ID ▪ Lower risk of ID error ▪ Aerial view permits accuracy not available by ground
Comments	▪ Police can support fire and EMS ▪ Visibility increased to 360 degrees ▪ Reduction in human error ▪ Reinforces/redefines incident command response	▪ Streamlines multi-agency investigation ▪ Ensures greater command and control in area wide operations

APPENDIX 2

Summary of UAS Legislation

Table 4. UAS legislation enacted 2016, by state

State	Legislation enacted in 2016
1. Alabama	
2. Alaska	HB 256
3. Arizona	SB 1449
4. Arkansas	
5. California	
6. Colorado	
7. Connecticut	
8. Delaware	
9. Florida	
10. Georgia	
11. Hawaii	
12. Idaho	SB 1213
13. Illinois	HB 5808
14. Indiana	HB 1013; HB 1246
15. Iowa	
16. Kansas	SB 319; SB 249
17. Kentucky	
18. Louisiana	HB 19; HB 335; HB 634; SB 141
19. Maine	
20. Maryland	
21. Massachusetts	
22. Michigan	
23. Minnesota	
24. Mississippi	
25. Missouri	
26. Montana	
27. Nebraska	
28. Nevada	
29. New Hampshire	
30. New Jersey	
31. New Mexico	
32. New York	
33. North Carolina	

34. North Dakota	
35. Ohio	
36. Oklahoma	HB 2599
37. Oregon	HB 4066; SB 5702
38. Pennsylvania	
39. Rhode Island	HB 7511; SB 3099
40. South Carolina	
41. South Dakota	
42. Tennessee	SB 2106; HB 2376
43. Texas	
44. Utah	HB 126; HB 3003
45. Vermont	SB 155
46. Virginia	HB 412; HB 29; HB 30
47. Washington	
48. West Virginia	
49. Wisconsin	SB 338; AB 670
50. Wyoming	

Source: NCSL 2016.

Table 5. UAS legislation enacted 2013–2015, by state

State	Enacted in 2013	Enacted in 2014	Enacted in 2015
1. Alabama			
2. Alaska		HB 255	
3. Arizona			
4. Arkansas			HB 1349; HB 1770
5. California			AB 856
6. Colorado			
7. Connecticut			
8. Delaware			
9. Florida	SB 92		SB 766
10. Georgia			
11. Hawaii	SB 1221		SB 661
12. Idaho	SB 1134		
13. Illinois	SB 1587; HB 1652	SB 2937	SB 44
14. Indiana		HB 1009	
15. Iowa		HF 2289	
16. Kansas			
17. Kentucky			
18. Louisiana		HB 1029	SB 183
19. Maine			LD 25
20. Maryland	HB 0100/CH 0423		SB 370
21. Massachusetts			

Table 5. UAS legislation enacted 2013–2015, by state

State	Enacted in 2013	Enacted in 2014	Enacted in 2015
22. Michigan			SB 54
23. Minnesota			
24. Mississippi			SB 2022
25. Missouri			
26. Montana	SB 196		
27. Nebraska			
28. Nevada	AB 507		AB 239
29. New Hampshire			SB 222
30. New Jersey			
31. New Mexico			
32. New York			
33. North Carolina	SB 402	SB 744	SB 446
34. North Dakota			HB 1328
35. Ohio		HB 292	
36. Oklahoma			
37. Oregon			HB 2534
38. Pennsylvania			
39. Rhode Island			
40. South Carolina			
41. South Dakota			
42. Tennessee		SB 1777; SB 1892	HB 153
43. Texas			HB 3628
44. Utah		SB 167	HB 296
45. Vermont			
46. Virginia			HB 2125; HB 1301
47. Washington			
48. West Virginia			HB 2515
49. Wisconsin		AB 203; SB 196	
50. Wyoming			

Sources: McKenna 2014b, NCSL 2015a, NCSL 2015b.

Table 6. Currently enacted UAS legislation applicable to police, 2013–2015

State	Enacted legislation	Addressing admissibility
1. Alabama		
2. Alaska	HB 255	
3. Arizona		
4. Arkansas		
5. California		
6. Colorado		
7. Connecticut		
8. Delaware		
9. Florida	SB 92	SB 92
10. Georgia		
11. Hawaii		
12. daho	SB 1134	
13. Illinois	SB 1587; HB 1652; SB 2937	SB 1587
14. Indiana	HB 1009	HB 1009
15. Iowa	HF 2289	HF 2289
16. Kansas		
17. Kentucky		
18. Louisiana		
19. Maine	LD 25	
20. Maryland		
21. Massachusetts		
22. Michigan		
23. Minnesota		
24. Mississippi		
25. Missouri		
26. Montana	SB 196	SB 196
27. Nebraska		
28. Nevada	AB 239	AB 239
29. New Hampshire		
30. New Jersey		
31. New Mexico		
32. New York		

Table 6. Currently enacted UAS legislation applicable to police, 2013–2015

State	Enacted legislation	Addressing admissibility
33. North Carolina	SB 402; SB 744	
34. North Dakota		
35. Ohio		
36. Oklahoma		
37. Oregon	HB 2710	HB 2710
38. Pennsylvania		
39. Rhode Island		
40. South Carolina		
41. South Dakota		
42. Tennessee	SB 796; HB 1952; SB 1777	SB 796
43. Texas	HB 912; HCR 217	
44. Utah	SB 167; HB 296	
45. Vermont		
46. Virginia	HB 2012; SB 1331; HB 2125; SB 1301	HB 2125; SB 1301
47. Washington		
48. West Virginia		
49. Wisconsin		
50. Wyoming		

Sources: McKenna 2014b, NCSL 2015a NCSL 2015b.

APPENDIX 3

Checklist for Planning and Implementation of a Law Enforcement sUAS Program

Conduct background research

1. Research and select the sUAS system that fits with program's mission.
   - ☐ Consider all possible benefits and challenges.
2. Lay the legal groundwork.
   - ☐ Research the legal environment in your jurisdiction and work with city attorney/DA to lay out legal grounds for use and restrictions to protect privacy, civil rights, and First Amendment protected activities.
   - ☐ Research system requirements for acquiring and storing relevant data collected.
   - ☐ Research potential issues regarding public access to the data captured with UAS, including open records and Freedom of Information Act requirements, discovery obligations, and Privacy Act restrictions that may require sophisticated editing to blur faces or other identifying characteristics of individuals appearing in the videos.
   - ☐ Begin to research the Federal Aviation Regulations related to civil and public sUAS operations.
   - ☐ Consider developing a privacy impact assessment or something similar. Accept that privacy concerns will be a major source of opposition, and confront them directly. A Privacy Impact Assessment (PIA) is a decision making tool used to identify and mitigate privacy risks at the beginning and throughout the development life cycle of a program or system. PIAs help the public understand what information is being collected and how it will be used, shared, accessed and stored.

Conduct a needs assessment

3. Determine whether your community is ready for a sUAS, a critical component of a needs assessment.
   - ☐ Gather community and stakeholder input around the issue and build dialogue around the sUAS with the community, policymakers, and other stakeholders such as state lawmakers.
   - ☐ Ensure that policymakers and the public are aware of the parameters of the system and who will have access to the data and under what circumstances.
   - ☐ Conduct cost-benefit research or identify research demonstrating that a sUAS is an appropriate and cost effective method for addressing the law enforcement purpose for which it will be used.
   - ☐ Include the findings from legal research, cost-benefit research, and community and stakeholder input in the final determination of need.

Planning and preparation

4. Develop a written operating/working plan for the sUAS.
   - ☐ Define under what circumstances the sUAS will be used; how the team will ensure procedures are followed; measures to ensure operating safety; measures to ensure privacy and civil rights protections; when a warrant will be sought; and procedures for operations that do not require warrant.
5. Develop formal departmental sUAS policies and procedures.

6. Assemble sUAS Team/Crew.
   - ☐ Identify supervising officer, pilot in command (PIC) or operator, and observer. Also consider other crew members such as a video sensor operator.
   - ☐ Begin operational training.
7. Present plans for the sUAS to policymakers, public and media.
   - ☐ Establish community-focused approach to transparency and engagement, making it clear that the department has considered and laid plans to protect safety and privacy.
   - ☐ Modify these plans as necessary in response to feedback from policy makers and the public.

Implementation and maintenance

8. Acquire sUAS.
   - ☐ Continue training
   - ☐ Provide public updates on training and development progress.
   - ☐ Continue outreach with community and stakeholder groups.
   - ☐ Set up system to evaluate program impact.
9. Complete training and fully implement sUAS operations.
   - ☐ Announce completion of training and operational status to public.
   - ☐ Ensure all sUAS policies and procedures are followed.
   - ☐ Evaluate program impact.
10. Maintain continued sUAS communication.
    - ☐ Maintain internal notification protocol to ensure departmental staff, particularly the Public Information Officer, knows of sUAS operations.
    - ☐ Provide regular reports on sUAS operations to the public, with reminder of how safety and privacy are being protected. Plan for major public announcements when the sUAS is successfully deployed to benefit the public.
    - ☐ Publicly address any misuse, which will reinforce community confidence that oversight mechanisms are effective.
    - ☐ Establish procedure for periodically reviewing policy to address any lessons learned during implementation and use, particularly, if new uses are developed.

APPENDIX 4

Sample Press Release

Gotham City Police Department
James Gordon, Commissioner

For immediate release: January 1, 2016
Contact: Bob Kane, PIO, (000) 000-0000

Gotham City Police Department to Hold Public Information Meeting on Unmanned Aerial Systems

The Gotham City Police Department will hold a public meeting on Thursday, Jan. 12 on how unmanned aerial systems can benefit the public and improve officer safety.

The meeting will be held at the Alfred Pennyworth Community Center from 7:30 to 9:30 p.m.

This meeting will be the first of a series that will be held around the city to provide information and seek public input on the proposed plan to acquire an unmanned aerial system for the GCPD.

"I look forward to meeting with our citizens and explaining how valuable an unmanned aerial system would be to our efforts to ensure public safety," Commissioner James Gordon said. "We also want the public to understand the protocols we are putting in place to protect privacy."

The Gotham City Police Department has been researching the potential benefits of an unmanned aerial system, which many in the public and media refer to as "drones." The department has drawn up a detailed plan of how such an aircraft would be used, and the safeguards that will be put in place to ensure both safe flying practices and protection of privacy.

Commissioner Gordon said he expects the public will be supportive of the possible uses of the unmanned aerial system, which include searching for lost citizens, aiding officers in quickly clearing accident scenes to cut down on traffic delays, checking for damage and victims after a natural disaster, and providing officers a means of determining whether criminals may be hiding in wait to attack.

The unmanned aerial system would provide the Gotham City Police Department with many of the capabilities of a manned helicopter unit at a fraction of the cost, Commissioner Gordon said.

The plan's details include the following:

- The aircraft will weigh less than 25 pounds (as required by the Federal Aviation Administration) and fly no higher than 400 feet.
- It will be equipped with a camera and infrared sensors, but absolutely will NOT be equipped with weapons of any sort.
- It will always be in control of a trained four-member crew, and any missions will be approved by a captain after careful review.
- The aircraft will NOT be used for general surveillance.
- Data gathered by the aircraft's camera and sensors will not be permanently stored except when necessary as part of an investigation. Data used in investigations will be erased once it is no longer needed.

For more information on the proposal to purchase an unmanned aerial system, visit the Gotham City Police Department website or its Facebook and Twitter accounts.

###

APPENDIX 5

Mesa County (Colorado) Sheriff's Office UAS FAQs

MSCO Unmanned Aircraft System Team

Frequently Asked Questions

What is a "Drone?" Some of the first radio controlled airplanes (drones) were developed in the 1930's by the Radioplane Company. The military used these aircraft as flying targets to train and hone the skills of anti-aircraft gunners. During World War II, the Radioplane Corporation produced over 15,000 of these aircraft for the U.S. Army.

Since then technology has improved greatly, and although the term "drone" is still commonly used in the military, we prefer to use the more current, and more descriptive term, "Unmanned Aircraft System" or UAS.

How do they work? Very simply stated UAS fly using a sophisticated autopilot system that assists the pilot when flying the aircraft manually, or has the ability to fly the aircraft by itself using a pre-loaded flight plan designed by the pilot for that specific mission.

Our aircraft are powered by a clean, efficient battery system, and during flight the aircraft sends a constant stream of information to the pilot indicating the altitude, heading, bearing, airspeed, position, battery levels and a live video feed from the aircraft mounted camera system. If there is a loss of communication or the batteries are getting too low, the aircraft has the ability to execute a "fail safe" procedure and automatically return to the point of take-off for landing or gently land immediately.

How many UAS do you have? We operate two different electric powered systems.

The first is a Draganflyer X4-ES helicopter that weighs about five pounds. The second system is a fixed wing airplane called the Falcon. The Falcon UAS weighs about nine pounds, is launched by hand for take-off and uses a brightly colored parachute when landing.

Many people ask us "why both"? We originally started our program flying the Draganflyer helicopter system. The helicopter is excellent for small operations and capturing aerial documentation of a crime scene or serious auto accident, but the helicopter is not very effective in covering large search areas.

To cover a large area we implemented the Falcon fixed wing aircraft because the plane flies faster, longer, and serves as an excellent tool when searching a large area or quickly used to create detailed 3D aerial computer models of these large areas.

What kind of UAS aircraft are available to Law Enforcement? There are helicopters and airplanes of all sizes available and as you can imagine, the cost of these systems varies greatly between size and capability.

The large systems currently available are much too expensive and are not necessary for our use.

Mesa County Sheriff's Office Grand Junction Colorado Sheriff Rebecca Spiess

Draganflyer X4-ES UAS

Falcon UAS Launch

Do other Law Enforcement Agencies operate UAS? Yes, but the numbers are very low. Of the 19,000 agencies in the United States, we estimate less than ten agencies are actively pursuing FAA approval and/or utilizing UAS.

How do you use your UAS aircraft? We most often use UAS for crime scene photography or search and rescue missions.

With aerial crime scene photography we can quickly photograph and build three dimensional models that are useful for investigators, prosecutors, and juries.

In search and rescue missions, aerial views are self explanatory but can be enhanced with the use of infrared technology which allows us to see anything with a heat signature.

While less frequent, we have used our systems to help locate dangerous fugitives in wooded areas and assisted county arson investigators in identifying heat sources within structure fires.

How often do you use the UAS? Our first mission was in October 2008. We fly on an "as needed basis". Since 2008 we've flown just over 55 missions not including training flights.

How much do they cost? We've spent less than $25,000.00, on our entire program. As one of the first public safety agencies in the United States to explore this technology we had the opportunity to work with vendors to Beta test and implement these systems for little or no money.

However, the actual retail price would be in the range of $25,000.00 to $50,000.00, per system.

UAS operating costs at this time are very low for our agency, but in order to project long term operating cost to include replacement parts, batteries, etc., we have projected a $25.00 an hour UAS operating cost (as a reasonable rate).

In contrast, manned aviation can cost hundreds to thousands of dollars per hour.

We feel the relatively low system cost and on-going operational cost is the largest driver behind utilizing this aerial technology.

What restrictions are in place to protect citizen's civil liberties and privacy concerns? Historically, law enforcement has had the ability to have an aerial view with manned aircraft for many decades. As a result, case law has been established that guides our use of the aircraft. There is no effort here to somehow use the UAS to circumvent well established 4th Amendment protections.

The technology in the UASs is appropriately limited. For example, our equipment does not allow us to see through walls, listen to conversations, monitor cell phones, etc. Our unmanned systems are mission and incident

Mesa County Sheriff's Office Grand Junction Colorado Sheriff Rebecca Spiess

Mesa County (Colorado) Sheriff's Office UAS FAQs, continued

driven only. Images collected with the use of this technology are handled and retained within public safety standards, consistent with images collected with any camera by law enforcement and are subject to professional standards, codes of conduct, case law, and with the public's trust in mind.

Can you legally fly over my backyard and do you need a warrant? Yes, we can legally fly our UAS over your backyard with the same guidelines used by manned aviation applying.

However, if during the course of an investigation the subject of a search is your backyard, we have taken the position as an agency to seek a warrant or consent from the property owner until case law specific to UAS, can be established.

Do your systems carry weapons? No. In our experience, and opinion, there is no use for weapons onboard UAS in civilian law enforcement.

Can your UAS be hacked with the controls taken over by someone else? No. The control data that travels through the air is encrypted. In addition, safeguards are in place so that if the technology fails, the aircraft either returns to the original point of take-off for landing or slowly descends to the ground.

Can the Mesa County Sheriff's Office be hired by a local resident or business to fly the systems for commercial use? No. This would violate our flight approvals from the Federal Aviation Administration.

What is driving the use of UAS in law enforcement? Through years of use, UAS have demonstrated to be a practical, cost effective alternative to manned aviation.

We have identified two core missions in crime scene photography, and search and rescue. However, the primary driving factor is the fact that these systems cost us just $25.00 per hour to operate as compared to $400.00 to $1,200.00 an hour for manned aviation. We have hired helicopters in the past for search and rescue missions and paid $650.00 an hour.

Do you have UAS Policy and Procedures or other guidance documents you operate under? Yes, as recommended with any tool used by law enforcement, use of a UAS is within the guidelines of a robust policy.

What training do your pilots have? Our pilots have received training from the manufacturer of each system, as well as instruction from our experienced instructional staff. And like all critical training we schedule our pilots to complete recurring UAS proficiency training.

Please note, the FAA has not released any guidelines for pilot certification for UAS, and as a result, our current curriculum has been developed in-house based around industry standards.

We are actively working with the FAA to develop a standardized UAS operations course which will become required training for all UAS pilots at the Mesa County Sheriff's Office, and very possibly this work will be adopted by public safety U.S. wide.

Do you have FAA approval to operate UAS or is it required? Yes, FAA flight approval is required and the Mesa County Sheriff's Office has been granted flight approval by the FAA to fly anywhere inside Mesa County, Colorado, daytime, no higher than 400 feet above the ground without flying any closer than five miles to the Grand Junction Regional Airport.

The official document is referred to as a Certificate of Authorization/Waiver (COA). It is the approval process by which the Federal Aviation Administration allows for public agencies (divisions of government) to operate UAS in the national airspace given there are no current regulations in place for UAS operations. For more information about the Certificate of Authorization process please contact Dave Morton with the FAA at david.morton@faa.gov.

Mesa County Sheriff's Office Grand Junction Colorado Sheriff Rebecca Spiess

What are the rules governing the use of UAS at Mesa County? To fly legally any public agency in the United States must obtain a Certificate of Authorization/Waiver (COA).

This certificate comes after a significantly invasive process whereby the FAA evaluates everything from the training and medical condition of the UAS pilots to the specific systems and airspace you can fly in.

Along with providing numerous safety procedures addressing UAS operations, any agency is required to do an airworthiness assessment of the specific systems they intend to fly.

Can citizens buy their own UAS and fly them? Yes. As long as the use is for hobby/recreation the requirements are far less strict than for civilian law enforcement.

The professional use of UAS for monetary gain is currently prohibited given the lack of any specific regulation from the FAA.

With that said however, as you see in the news and Internet, professional use of UAS for monetary gain is actually very widespread.

For example the real estate industry, aerial video production, survey work, and agriculture are commercial uses currently capitalizing on UAS. There are an estimated 50,000 UAS users currently flying in the United States.

What are the projected economic impacts of using UAS in the United States? By some estimates it is projected that in the first three years of integration into the National Airspace more than 70,000 jobs will be created in the United States with an economic impact of more than $13.6 billion.

This benefit will grow through 2025 when more than 100,000 jobs are created and economic impact of $82 billion.

More specifically, as the Mesa County Sheriff's Office has had the opportunity to build a professional, publicly trusted and accepted UAS program. Mesa County has extensive UAS experience and is an attractive location to the UAS industry as a result of that work. This work will play a key role in attracting the industry and have a potential economic impact on the local area.

Members of the UAS team have been invited to both the Colorado State Capitol and Washington, D.C., to speak to members of government, as well as numerous speaking engagements throughout the country as to the benefits of small UAS.

This, as well as numerous national and international media highlights (National Geographic, TIME Magazine, NBC Nightly new, FOX, CNN) has made our UAS program very visible to the public which will be an advantage in attracting UAS business to Mesa County.

How do you go about sharing this technology with the community? For several years now we have been taking the systems to the annual "Mesa County Safety Fair". Our UAS team is on-hand to showcase the aircraft, answer questions and it provides an excellent opportunity for people to see the systems up close.

Mesa County Sheriff UAS on display at the Mesa County Safety Fair 2014

APPENDIX 6

Arlington (Texas) Police Department UAS FAQs

Arlington (TX) Police Department FAQs

The Arlington Police Department recently received approval from the Federal Aviation Administration (FAA) to fly its two small battery-operated, remotely-controlled helicopters after two years of planning and training. This additional tool is one of many public safety options available to police officers in the ongoing effort to keep Arlington residents and visitors safe. In an effort to help foster a better understanding of the Aviation Unit, when and how it will be operated, and to clarify the aircraft's capabilities, this web page was created.

How will the police department utilize the Aviation Unit?
They will be used in a variety of public safety applications such as helping us find missing persons, clear major traffic crashes more quickly, aid in assessing damages and losses from natural disasters like floods and tornadoes, and take forensic photographs of complex crime scenes. Our helicopters will NOT be used in car pursuits, issue traffic citations, carry weapons or be used for routine patrols and surveillance.

What are the specifics of the equipment used by the Aviation Unit?
Arlington purchased two small helicopters using federal grant funds. They are battery-operated helicopters that carry consumer grade camera/video equipment and are best suited for situations that require less than an hour flight time due to battery limitations. Each aircraft weighs 11 pounds, is approximately 58 inches long, and 20 inches high.

When and where can the Aviation Unit fly?
At this point, the aircraft can only be flown during daylight hours and less than 400 feet above ground. The small helicopter must be flown within line of sight of the officer who is remotely piloting the helicopter, which essentially means it must be flown in the general area where it takes off. The equipment has to be driven to the incident scene and unloaded after a clearly defined incident perimeter has been established. The police department is not allowed to fly directly over crowds such as football games or parades. Flying north of Interstate Highway 30 is also currently prohibited due to the proximity to the Dallas/Fort Worth International Airport.

Why purchase small helicopters instead of larger, more commonly used helicopters?
Unmanned aircraft technology provides an alternative to traditional aviation for law enforcement agencies. Unmanned or remotely piloted aircraft are much cheaper to own and operate than

traditional fixed-wing planes and helicopters. Although our small helicopters look similar to hobby aircraft, they are equipped with more sophisticated navigation and communication equipment that allows for safer and more reliable operations and are operated under different FAA regulations.

Who makes the final decision on whether the Aviation Unit is used?

APD has established specific procedures for when and how the unmanned systems can be used. All flights are pre-approved by a command level officer. Officers trained as pilots and safety observers maintain all flight and maintenance records. Notices are issued through the FAA to alert other pilots in the area. They are flown within clearly defined incident perimeters.

Will my privacy be impacted?

No, your privacy will not be impacted. Maintaining an individual's privacy and protecting the civil liberties of all persons is of paramount importance to the department. The Arlington Police Department is bound by federal law and the laws of the State of Texas that direct the use of helicopters of all types and sizes, as it relates to the privacy of citizens. This same case law that applies to manned-helicopter programs that are used in many urban police departments across the country is the same case law that applies to these unmanned systems as well. Both statutory laws and case laws dictate when search warrants must be obtained and provides limits on the use of technology by law enforcement to investigate suspected criminal activity in our community. In other words, if a search warrant is needed to access private property now such as looking in a backyard, then a search warrant would also be needed for accessing private property with our small helicopter. Again, our helicopter program will not be used for arbitrary surveillance and must comply with all federal regulations and laws.

Arlington Police Department UAS Use Report

City of Arlington Police Department

REPORT FOR THE USE OF SMALL UNMANNED AIRCRAFT SYSTEMS

January 1, 2013 – December 31, 2014

City of Arlington Police Department

Report for the Use of Small Unmanned Aircraft Systems

January 1, 2013 through December 31, 2014

This document satisfies the reporting requirements mandated by H.B. 912 related to the use of unmanned aircraft.

Background:

In 2013, the 83rd Texas Legislature passed H.B. 912. The bill requires that no earlier than January 1 and not later than January 15 of each odd-numbered year, a municipal law enforcement agency located in a county or municipality 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.

The Arlington Police Department (APD) is authorized by the Federal Aviation Administration to operate two 11-pound battery-powered helicopters and conducted flights during the reporting period. In accordance with H.B. 912, this report includes:

- number of times the unmanned aircraft was used, organized by date, time, location, and the types of incidents and types of justification for the use;
- number of criminal investigations aided by the use of the unmanned aircraft and a description of how the unmanned aircraft aided each investigation;
- number of times the 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;
- 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
- total cost of acquiring, maintaining, repairing, and operating or otherwise using each unmanned aircraft for the preceding 24 months.

In addition, the APD retains the report for public viewing at its headquarters located at 620 W. Division Street in Arlington, Texas and has posted the report on the department's publicly accessible website at www.arlingtonpd.org.

Arlington Police Department UAS Use Report, continued

City of Arlington Police Department
Report for the Use of Small Unmanned Aircraft Systems
January 1, 2013 through December 31, 2014

Date	Time	Location	Incident Type	Justification	Description	Type and frequency of information collected on an individual, residence, property, or area which was not the subject of an LE operation
1/15/2013	13:00	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training*	N/A
1/16/2013	13:00	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
2/5/2013	13:00	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
2/7/2013	11:11	5500 Lake Arlington Dam	Training	Training	FAA on-site inspection for Certificate of Authorization approval	N/A
2/11/2013	16:24	5500 Lake Arlington Dam	Training	Training	Initial pilot training for pilot certification on UAS platform	N/A
2/13/2013	9:55	5500 Lake Arlington Dam	Training	Training	Initial pilot training for pilot certification on UAS platform	N/A
2/14/2013	10:15	5500 Lake Arlington Dam	Training	Training	Initial pilot training for pilot certification on UAS platform	N/A
3/19/2013	16:05	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
3/28/2013	13:14	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
5/13/2013	11:13	1600 W. Park Row Dr	Fatal Crash	Official Investigation	Video of vehicles involved in fatal traffic crash and of resulting debris field	N/A
5/24/2013	9:40	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
6/7/2013	12:50	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
6/28/2013	10:10	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
7/12/2013	10:26	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
8/9/2013	11:30	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
8/16/2013	11:45	5500 Lake Arlington Dam	Training	Training	Test flight to ensure proper functioning of repaired control surface area	N/A
8/23/2013	10:45	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
9/17/2014	14:00	5500 Lake Arlington Dam	Training	Training	Ground Station flight training	N/A
9/18/2013	10:58	5500 Lake Arlington Dam	Training	Training	Ground Station flight training	N/A
9/19/2013	9:37	5500 Lake Arlington Dam	Training	Training	Ground Station flight training	N/A
10/25/2013	11:30	5500 Lake Arlington Dam	Training	Training	Joint training with APD traffic unit	N/A
10/28/2013	11:30	1135 Silverwood Dr	Tactical Event	Official Investigation	Patrol responded to a shooting call where the suspect shot and killed someone in an apartment parking lot and then barricading himself. Based upon the suspect having a rifle, UAS was used to search for other victims within the suspect's line of fire. Our SWAT Team was able to collect vital intelligence without going into harm's way to bring suspect into custody.	N/A

City of Arlington Police Department
Report for the Use of Small Unmanned Aircraft Systems
January 1, 2013 through December 31, 2014

Date	Time	Location	Incident Type	Justification	Description	Type and frequency of information collected on an individual, residence, property, or area which was not the subject of an LE operation
11/8/2013	11:13	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
12/12/2013	11:30	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
1/24/2014	11:15	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training*	N/A
2/28/2014	11:13	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
3/28/2014	10:36	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
4/14/2014	11:25	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A
10/3/2014	11:00	1207 California Ln	Training	Training	Test flight on UAS	N/A
10/3/2014	15:30	3001 W. Division St.	Storm Damage Assessment	Assess storm damage	The storm system destroyed buildings across the city in three different zones and there were widespread power outages that lasted for days. The Arlington Emergency Operation Center requested video of damaged area for storm path assessment so that proper allocation of city resources could be matched to the hardest hit areas.	Video storm damage
10/3/2014	15:55	2111 W. Division St.	Storm Damage Assessment	Assess storm damage	Arlington Emergency Operation Center requested video of damaged area for storm path assessment	Video storm damage
10/6/2014	14:24	1100 S. Pecan St.	Storm Damage Assessment	Assess storm damage	Arlington Emergency Operation Center requested video of damaged area for storm path assessment	Video storm damage
10/6/2014	15:26	1600 Industrial Dr.	Storm Damage Assessment	Assess storm damage	Arlington Emergency Operation Center requested video of damaged area for storm path assessment	Video storm damage
10/16/2014	11:04	5500 Lake Arlington Dam	Training	Training	Test flight on repaired UAS that was damaged during training	N/A
11/14/2014	11:12	5500 Lake Arlington Dam	Training	Training	FAA Monthly currency training	N/A

Normal Currency Training is defined as an FAA requirement training flight. All FAA licensed pilots are required to maintain their flight currency by completing flights to include at least three take off's and three landing's within the previous rolling 90-day period.

Arlington Police Department UAS Use Report, continued

City of Arlington Police Department
Report for the Use of Small Unmanned Aircraft Systems
January 1, 2013 through December 31, 2014

Costs	Reporting Period	Description
Acquisition	$3,888.08	Tablets to store all required flight documents, checklists, standard operating procedures, weather applications, and flight log applications.
Maintenance	$4,194.45	Replacement batteries for helicopters.
Repairs	$376.07	Costs related to shipping helicopter back to vendor for repairs
Operations	$0.00	No expenses
Training	$8,822.98	Certification training of Ground Station and Auto Pilot Operation for all pilots.
Medical Certifications	$600.00	Medical Licenses for pilots.
Other	$3,628.03	Communication equipment and public education display equipment
Total	$12,651.01	

APPENDIX 8

International Association of Chiefs of Police (IACP) 2012 UAS Guidelines

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 our 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.

International Association of Chiefs of Police (IACP) 2012 UAS Guidelines, continued

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. **UA Flight Crewmember** - A pilot, visual observer, payload operator or other person assigned duties for a UA 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, that 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 UA 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 (COA) 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. UA 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.

APPENDIX 9

Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations

U.S. Department of Transportation
Federal Aviation Administration

LAW ENFORCEMENT GUIDANCE FOR SUSPECTED UNAUTHORIZED UAS OPERATIONS

Issue

There is evidence of a considerable increase in the unauthorized use of small, inexpensive Unmanned Aircraft Systems (UAS) by individuals and organizations, including companies. The FAA retains the responsibility for enforcing Federal Aviation Regulations, including those applicable to the use of UAS. The agency recognizes though that State and local Law Enforcement Agencies (LEA) are often in the best position to deter, detect, immediately investigate,[1] and, as appropriate,[2] pursue enforcement actions to stop unauthorized or unsafe UAS operations. The information provided below is intended to support the partnership between the FAA and LEAs in addressing these activities.

Discussion

The general public, a wide variety of organizations, including private sector (e.g., commercial companies), non-governmental (e.g., volunteer organizations), and governmental entities (e.g., local agencies) continue to demonstrate significant interest in UAS. The benefits offered by this type of aircraft are substantial and the FAA is committed to integrating UAS into the National Airspace System (NAS). This introduction, however, must address important safety and security considerations. The increasing number of cases of unauthorized use of UAS is a serious concern for the FAA and, in terms of safety and security challenges, many of its interagency partners.

This document is intended to assist LEAs in understanding the legal framework that serves as the basis for FAA legal enforcement action against UAS operators for unauthorized and/or unsafe UAS operations (Section 1) and to provide guidance regarding the role of LEAs in deterring, detecting, and investigating unauthorized and/or unsafe UAS operations (Section 2).

SECTION 1.

Basic Legal Mandates

The FAA's safety mandate under 49 U.S.C. § 40103 requires it to regulate aircraft operations conducted in the NAS,[3] which include UAS operations, to protect persons and property on the

[1] At least in terms of initial contact with the suspected offender.
[2] Applying any laws falling within the enforcement authority of the LEA in question.
[3] The NAS is "the common network of U.S. airspace; air navigation facilities, equipment and services, airports or landing areas . . . . Included are system components shared jointly with the military." See FAA Pilot/Controller Glossary (Apr. 3, 2014), available at http://www.faa.gov/air_traffic/publications/media/pcg_4-03-14.pdf.

ground, and to prevent collisions between aircraft and other aircraft or objects. In addition, 49 U.S.C. § 44701(a) requires the agency to promote safe flight of civil aircraft in air commerce by prescribing, among other things, regulations and minimum standards for other practices, methods, and procedures the Administrator finds necessary for safety in air commerce and national security.[4]

A UAS is an Aircraft that Must Comply with Safety Requirements

A UAS is an "aircraft" as defined in the FAA's authorizing statutes and is therefore subject to regulation by the FAA. 49 U.S.C. § 40102(a)(6) defines an "aircraft" as "any contrivance invented, used, or designed to navigate or fly in the air." The FAA's regulations (14 C.F.R. § 1.1) similarly define an "aircraft" as "a device that is used or intended to be used for flight in the air." Because an unmanned aircraft is a contrivance/device that is invented, used, and designed to fly in the air, it meets the definition of "aircraft." The FAA has promulgated regulations that apply to the operation of all aircraft, whether manned or unmanned, and irrespective of the altitude at which the aircraft is operating. For example, 14 C.F.R. § 91.13 prohibits any person from operating an aircraft in a careless or reckless manner so as to endanger the life or property of another.

Model Aircraft Operations

An important distinction to be aware of is whether the UAS is being operated for hobby or recreational purposes or for some other purpose. This distinction is important because there are specific requirements in the FAA Modernization and Reform Act of 2012, Public Law 112-95, (the Act) that pertain to "Model Aircraft" operations, which are conducted solely for hobby or recreational purposes. While flying model aircraft for hobby or recreational purposes does not require FAA approval, all model aircraft operators must operate safely and in accordance with the law. The FAA provides guidance and information to individual UAS operators about how they can operate safely under current regulations and laws. Guidance may be found at: http://www.faa.gov/uas/publications/model_aircraft_operators/

Section 336(c) of the Act defines "Model Aircraft" as 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.

Each element of this definition must be met for a UAS to be considered a Model Aircraft under the Act. Under Section 336(a) of the Act the FAA is restricted from conducting further rulemaking specific to Model Aircraft as defined in section 336(c) so long as the Model Aircraft operations are conducted in accordance with the requirements of section 336(a). Section 336(a) requires that—

[4] FAA action on these security concerns support and are informed by the national defense, homeland security, and law enforcement statutory responsibilities and authorities of our interagency partners.

Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations, continued

(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)).

Model Aircraft that Operate in a Careless or Reckless Manner

Section 336(b) of the Act, however, makes clear that the FAA has the authority under its existing regulations to pursue legal enforcement action against persons operating Model Aircraft when the operations endanger the safety of the NAS, even if they are operating in accordance with section 336(a) and 336(c). So, for example, a Model Aircraft operation conducted in accordance with section 336(a) and (c) may be subject to an enforcement action for violation of 14 C.F.R. § 91.13 if the operation is conducted in a careless or reckless manner so as to endanger the life or property of another.

UAS Operations that are not Model Aircraft Operations

Operations of UAS that are not Model Aircraft operations as defined in section 336(c) of the Act and conducted in accordance with section 336(a) of the Act may only be operated with specific authorization from the FAA. The FAA currently authorizes non-hobby or recreational UAS operations through one of three avenues:

(1) The issuance of a Certificate of Waiver or Authorization, generally to a governmental entity operating a public aircraft;

(2) The issuance of an airworthiness certificate in conjunction with the issuance of a Certificate of Waiver or Authorization; or

(3) The issuance of an exemption under part 11 of title 14, Code of Federal Regulations that relies on section 333 (Special Rules for Certain Unmanned Aircraft Systems) of the Act for relief from the airworthiness certificate requirement, also in conjunction with the issuance of a Certificate of Waiver or Authorization.

It is important to understand that all UAS operations that are not operated as Model Aircraft under section 336 of the Act are subject to current and future FAA regulation. At a minimum, any such flights are currently required under the FAA's regulations to be operated with an

authorized aircraft (certificated or exempted), with a valid registration number ("N-number"), with a certificated pilot, and with specific FAA authorization (Certificate of Waiver or Authorization).

Regardless of the type of UAS operation, the FAA's statutes and the Federal Aviation Regulations prohibit any conduct that endangers individuals and property on the surface, other aircraft, or otherwise endangers the safe operation of other aircraft in the NAS. In addition, States and local governments are enacting their own laws regarding the operation of UAS, which may mean that UAS operations may also violate state and local laws specific to UAS operations, as well as broadly applicable laws such as assault, criminal trespass, or injury to persons or property.

UAS Compliance with Airspace Security Requirements

As an aircraft, UAS operations (including those involving Model Aircraft) must be conducted in accordance with the airspace-centric security requirements prescribed by the FAA's regulations and various implementation tools used by the FAA, specifically including airspace with special flight rules and Notices to Airmen (NOTAM) that define Temporary Flight Restrictions (TFR). It is important that UAS operators and LEAs be familiar with the airspace restrictions respectively relevant to their operations and their enforcement area of responsibility.

Flight restrictions are used to protect, but are not limited to, special security events, sensitive operations (e.g., select law enforcement activity, space flight operations, etc.), and Presidential movement. The most up-to-date list of TFRs is available at http://tfr.faa.gov/tfr2/list.html.

See Attachment A for reference resources.[5]

SECTION 2.

The Role of Law Enforcement

The FAA promotes voluntary compliance by educating individual UAS operators about how they can operate safely under current regulations and laws. The FAA also has a number of enforcement tools available including warning notices, letters of correction, and civil penalties. The FAA may take enforcement action against anyone who conducts an unauthorized UAS operation or operates a UAS in a way that endangers the safety of the national airspace system. This authority is designed to protect users of the airspace as well as people and property on the ground.

However, as noted above, State and local Law Enforcement Agencies (LEA) are often in the best position to deter, detect, immediately investigate,[6] and, as appropriate,[7] pursue

[5] Attachment A also includes a NOTAM concerning avoidance (including no loitering) over power plants, dams, refineries, industrial complexes, and military facilities. Although not a restriction, this TFR urges aircraft operators to avoid these locations.
[6] At least in terms of initial contact with the suspected offender.
[7] Applying any laws falling within the enforcement authority of the LEA in question.

Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations, continued

enforcement actions to stop unauthorized UAS operations. Although the FAA retains the responsibility for enforcing FAAs regulations, FAA aviation safety inspectors, who are the agency's principal field elements responsible for following up on these unauthorized and/or unsafe activities, will often be unable to immediately travel to the location of an incident.

While the FAA must exercise caution not to mix criminal law enforcement with the FAA's administrative safety enforcement function, the public interest is best served by coordination and fostering mutual understanding and cooperation between governmental entities with law enforcement responsibilities. Although there are Federal criminal statutes that may be implicated by some UAS operations (see 49 U.S.C. § 44711), most violations of the FAA's regulations may be addressed through administrative enforcement measures. As with any other civil or criminal adjudication, successful enforcement will depend on development of a complete and accurate factual report contemporaneous with the event.

Although certainly not an exhaustive list, law enforcement officials, first responders and others can provide invaluable assistance to the FAA by taking the actions outlined below:

(1) **Witness Identification and Interviews.** Local law enforcement is in the best position to identify potential witnesses and conduct initial interviews, documenting what they observed while the event is still fresh in their minds. In addition, local law enforcement is in an optimum position to secure all information necessary for our safety inspectors to contact these witnesses in any subsequent FAA investigation. Administrative proceedings often involve very technical issues; therefore, we expect our own safety inspectors will need to re-interview most witnesses. We are mindful that in many jurisdictions, state law may prohibit the transmission of witness statements to third parties, including the FAA. In those circumstances it is extremely important that the FAA be able to locate and conduct independent interviews of these individuals.

(2) **Identification of Operators.** Law enforcement is in the best position to contact the suspected operators of the aircraft, and any participants or support personnel accompanying the operators. Our challenges in locating violators are marked in that very few of these systems are registered in any federal database and rarely will they have identifiable markings such as used for conventional manned aircraft. Likewise, information on few of the UAS operators will be archived in a pilot data base. Many operators advertise openly on the internet. However, in our enforcement proceedings, we bear the burden of proof, and showing who actually is operating the unmanned aircraft is critical. Therefore, evidentiary thresholds must be met even when using data or video acquired via the internet. Likewise, the purpose for the operation (such as in support of a commercial venture, to further some business interest, or to secure compensation for their services) may become an important element in determining what regulations, if any, may have been violated by the operation. Identification and interview of suspected operators early on will help immeasurably to advance enforcement efforts.

(3) **Viewing and Recording the Location of the Event.** Pictures taken in close proximity to the event are often helpful in describing light and weather conditions, any damage or injuries, and the number and density of people on the surface,

particularly at public events or in densely populated areas. During any witness interviews, use of fixed landmarks that may be depicted on maps, diagrams or photographs immeasurably help in fixing the position of the aircraft, and such landmarks also should be used as a way to describe lateral distances and altitude above the ground, structures or people (e.g. below the third floor of Building X, below the top of the oak tree located Y, anything that gives reference points for lay witnesses).

(4) **Identifying Sensitive Locations, Events, or Activities.** The FAA maintains a variety of security-driven airspace restrictions around the country to help protect sensitive locations, events, and activities through Temporary Flight Restrictions (TFR), Prohibited Areas, and other mechanisms such as the Washington, DC Flight Restricted Zone (DC FRZ). UAS operations, including Model Aircraft flights, are generally prohibited within these defined volumes of airspace. LEAs should become familiar with the steady-state airspace restrictions active within their area of responsibility, along with as-needed TFRs, which could be instituted to help protect sensitive events (e.g., major gatherings of elected officials) and activities (e.g., Presidential movements). If there is any question as to whether a TFR has been established in a given location, contact the nearest air traffic facility or flight service station for further information or visit http://tfr.faa.gov/tfr2/list.html for a graphic representation of TFRs locatable by state and effective dates.

(5) **Notification.** Immediate notification of an incident, accident or other suspected violation to one of the FAA Regional Operation Centers (ROC) located around the country is valuable to the timely initiation of the FAA's investigation. These centers are manned 24 hours a day, 7 days a week with personnel who are trained in how to contact appropriate duty personnel during non-business hours when there has been an incident, accident or other matter that requires timely response by FAA employees. A list of these centers and telephone numbers is included as Attachment B to this letter.

(6) **Evidence Collection.** Identifying and preserving any public or private security systems that may provide photographic or other visual evidence of UAS operations, including video or still picture security systems can provide essential evidence to the FAA. Many times these systems do not permanently store information but erase it as the system recycles at a given interval. Local law enforcement is in the best position to inquire and make initial requests to identify and preserve this form of evidence or obtain legal process for securing this evidence in the context of an investigation of a possible violation of state criminal law. In addition, some UAS may be marked with identification numbers ("N-numbers") signifying FAA registration. The presence or lack of these identification numbers may be significant in an FAA investigation. For example, an operator may state that he or she is conducting an approved commercial activity, which usually requires registered aircraft. However, the absence of registration markings on the UAS may indicate that the aircraft is not registered, meaning the operation may not be authorized. Note that identification numbers may not be conspicuous from a distance because of the size and non-traditional configuration of some UAS. The registered owners

Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations, continued

of UAS bearing identification numbers can be found by searching for the N-number on the FAA's website: www.faa.gov.

Virtually all of the items listed above are already in the tool box for law enforcement officers. Other investigative methods also may prove useful, such as consensual examination of the UAS, equipment trailers and the like. However, other law enforcement processes, such as arrest and detention or non-consensual searches almost always fall outside of the allowable methods to pursue administrative enforcement actions by the FAA unless they are truly a by-product of a state criminal investigation. We do not mean to discourage use of these methods and procedures where there is an independent basis for them under state or local law. We simply wish to emphasize that work products intended for FAA use generally should involve conventional administrative measures such as witness interviews, "stop and talk" sessions with suspected violators, consensual examination of vehicles and equipment, and other methods that do not involve court orders or the potential use of force by law enforcement personnel.

It is extremely difficult to provide a "one size fits all" guide to cooperative investigation of unauthorized UAS operations considering the myriad jurisdictions and the associated statutory and constitutional restraints and requirements. State and local officials are always urged to use their governmental unit's legal resources and their own management chain to develop acceptable protocols for dealing with these instances. In some situations, there may be legal bars to the sharing of some information or the use of databases designed for conventional law enforcement. However, with appropriate data collection during first responses and early reporting to the FAA, Federal, State and local agencies will be in the best position to both collect and share information that may be of interest to each jurisdiction. FAA aviation safety inspectors are adept at coordination with our own legal resources to ensure unauthorized operators are properly accountable for the potential risk they create to both people and property. In addition, we have specially trained inspectors within the FAA UAS Integration office who can provide expertise in this area.

If you have any questions or your agency would like to pursue advance planning on how to address these situations, please feel free to contact your local FAA Law Enforcement Assistance Special Agent or the FAA's Law Enforcement Assistance Program Office at (202) 267-4641 or (202) 267-9411.

8

Attachment A.

Excerpts

Presidential Movements

FDC 4/7607 ZBW RI..AIRSPACE PROVIDENCE, RHODE ISLAND..TEMPORARY FLIGHT RESTRICTIONS. OCTOBER 16, 2014 LOCAL. THIS NOTAM REPLACES NOTAM 4/7600 DUE TO SCHEDULE CHANGE. PURSUANT TO 49 USC 40103(B THE FEDERAL AVIATION ADMINISTRATION (FAA) CLASSIFIES THE AIRSPACE DEFINED IN THIS NOTAM AS 'NATIONAL DEFENSE AIRSPACE'. PILOTS WHO DO NOT ADHERE TO THE FOLLOWING PROCEDURES MAY BE INTERCEPTED DETAINED AND INTERVIEWED BY LAW ENFORCEMENT/SECURITY PERSONNEL. ANY OF THE FOLLOWING ADDITIONAL ACTIONS MAY ALSO BE TAKEN AGAINST A PILOT WHO DOES NOT COMPLY WITH THE REQUIREMENTS OR ANY SPECIAL INSTRUCTIONS OR PROCEDURES ANNOUNCED IN THIS NOTAM:
A) THE FAA MAY TAKE ADMINISTRATIVE ACTION, INCLUDING IMPOSING CIVI PENALTIES AND THE SUSPENSION OR REVOCATION OF AIRMEN CERTIFICATES; OR
B) THE UNITED STATES GOVERNMENT MAY PURSUE CRIMINAL CHARGES, INCLUDING CHARGES UNDER TITLE 49 OF THE UNITED STATES CODE, SECTION 46307; OR
C) THE UNITED STATES GOVERNMENT MAY USE DEADLY FORCE AGAINST THE AIRBORNE AIRCRAFT, IF IT IS DETERMINED THAT THE AIRCRAFT POSE AN IMMINENT SECURITY THREAT.
…
C. THE FOLLOWING OPERATIONS ARE NOT AUTHORIZED WITHIN THIS TFR: FLIGHT TRAINING, PRACTICE INSTRUMENT APPROACHES, AEROBATIC FLIGHT, GLIDER OPERATIONS, SEAPLANE OPERATIONS, PARACHUTE OPERATIONS, ULTRALIGHT, HANG GLIDING, BALLOON OPERATIONS, AGRICULTURE/CROP DUSTING, ANIMAL POPULATION CONTROL FLIGHT OPERATIONS, BANNER TOWING OPERATIONS, SIGHTSEEING OPERATIONS,MAINTENANCE TEST FLIGHTS, MODEL AIRCRAFT OPERATIONS, MODEL ROCKETRY, UNMANNED AIRCRAFT SYSTEMS (UAS), AND UTILITY AND PIPELINE SURVEY OPERATIONS.

Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations, continued

9

DC FRZ

FDC 0/8326 ZDC PART 1 OF 10 FLIGHT RESTRICTIONS, WASHINGTON, DC, EFFECTIVE 1012010401 UTC UNTIL FURTHER NOTICE. THIS NOTICE WILL REPLACE NOTAM 0/9477 DUE TO A CHANGE IN RESTRICTIONS. THIS NOTAM AND A NOTAM FOR THE LEESBURG MANEUVERING AREA SUPPLEMENT SUBPART V, 14 CFR PART 93 FOR THE WASHINGTON, D.C. SPECIAL FLIGHT RULES AREA (DC SFRA). PURSUANT TO 49 USC 40103(B), THE FAA HAS ESTABLISHED THE DC SFRA AREA AS 'NATIONAL DEFENSE AIRSPACE. ANY PERSON WHO DOES NOT COMPLY WITH THE REQUIREMENTS APPLICABLE TO THE DC SFRA MAY BE INTERCEPTED, DETAINED AND INTERVIEWED BY LAW ENFORCEMENT/SECURITY PERSONNEL. ANY OF THE FOLLOWING ADDITIONAL ACTIONS MAY ALSO BE TAKEN AGAINST A PILOT WHO DOES NOT COMPLY WITH THE REQUIREMENTS OR ANY SPECIAL INSTRUCTIONS OR PROCEDURES ANNOUNCED IN THIS NOTAM: A) THE FAA MAY TAKE ADMINISTRATIVE ACTION, INCLUDING IMPOSING CIVIL PENALTIES AND THE SUSPENSION OR REVOCATION OF AIRMEN CERTIFICATES; B) THE UNITED STATES GOVERNMENT MAY PURSUE CRIMINAL CHARGES, INCLUDING CHARGES UNDER TITLE 49 OF THE UNITED STATES CODE, SECTION 46307; C) THE UNITED STATES GOVERNMENT MAY USE DEADLY FORCE AGAINST THE AIRBORNE AIRCRAFT, IF IT IS DETERMINED THAT THE AIRCRAFT POSES AN IMMINENT SECURITY THREAT.

…

A. THE FOLLOWING OPERATIONS ARE NOT AUTHORIZED WITHIN THE DC FRZ: FLIGHT TRAINING, AEROBATIC FLIGHT, PRACTICE INSTRUMENT APPROACHES, GLIDER OPERATIONS, PARACHUTE OPERATIONS, ULTRA LIGHT, HANG GLIDING, BALLOON OPERATIONS, TETHERED BALLOONS, AGRICULTURE/CROP DUSTING, ANIMAL POPULATION CONTROL FLIGHT OPERATIONS, BANNER TOWING OPERATIONS, MAINTENANCE TEST FLIGHTS, MODEL AIRCRAFT OPERATIONS, MODEL ROCKETRY, FLOAT PLANE OPERATIONS, UNMANNED AIRCRAFT SYSTEMS (UAS) AND AIRCRAFT/HELICOPTERS OPERATING FROM A SHIP OR PRIVATE/CORPORATE YACHT. B. IT IS HIGHLY RECOMMENDED THAT A PILOT CONTINUOUSLY MONITOR VHF FREQUENCY 121.5 OR UHF FREQUENCY 243.0 FOR EMERGENCY INSTRUCTIONS WHEN OPERATING AN AIRCRAFT IN THE DC FRZ, EITHER IN AN AIRCRAFT THAT IS SUITABLY EQUIPPED, OR BY USE OF PORTABLE EQUIPMENT.

Avoidance of Power Plans Etc. *(Applied to all Aircraft, including UAS)*

FDC 4/0811 SPECIAL NOTICE. THIS IS A RESTATEMENT OF A PREVIOUSLY ISSUED ADVISORY NOTICE. IN THE INTEREST OF NATIONAL SECURITY AND TO THE EXTENT PRACTICABLE, PILOTS ARE STRONGLY ADVISED TO AVOID THE AIRSPACE ABOVE, OR IN PROXIMITY TO SUCH SITES AS POWER PLANTS (NUCLEAR, HYDRO-ELECTRIC, OR COAL), DAMS, REFINERIES, INDUSTRIAL COMPLEXES, MILITARY FACILITIES AND OTHER SIMILAR FACILITIES. PILOTS SHOULD NOT CIRCLE AS TO LOITER IN THE VICINITY OVER THESE TYPES OF FACILITIES.

10

Select Sporting Events

FDC 4/3621 FDC SPECIAL SECURITY NOTICE. SPORTING EVENTS. THIS NOTAM REPLACES FDC NOTAM 9/5151 TO REFLECT A TSA WEBSITE UPDATE AND ADDITIONAL INFORMATION CONCERNING AIRSPACE WAIVERS. FLIGHT RESTRICTIONS IN THIS NOTAM COMPLY WITH STATUTORY MANDATES DETAILED IN SECTION 352 OF PUBLIC LAW 108-7 AS AMENDED BY SECTION 521 OF PUBLIC LAW 108-199. PURSUANT TO 49 USC 40103(B), THE FEDERAL AVIATION ADMINISTRATION (FAA) CLASSIFIES THE AIRSPACE DEFINED IN THIS NOTAM AS 'NATIONAL DEFENSE AIRSPACE'. ANY PERSON WHO KNOWINGLY OR WILLFULLY VIOLATES THE RULES PERTAINING TO OPERATIONS IN THIS AIRSPACE MAY BE SUBJECT TO CERTAIN CRIMINAL PENALTIES UNDER 49 USC 46307. PILOTS WHO DO NOT ADHERE TO THE FOLLOWING PROCEDURES MAY BE INTERCEPTED, DETAINED AND INTERVIEWED BY LAW ENFORCEMENT/SECURITY PERSONNEL. PURSUANT TO 14 CFR SECTION 99.7, SPECIAL SECURITY INSTRUCTIONS, COMMENCING ONE HOUR BEFORE THE SCHEDULED TIME OF THE EVENT UNTIL ONE HOUR AFTER THE END OF THE EVENT. ALL AIRCRAFT OPERATIONS; INCLUDING PARACHUTE JUMPING, UNMANNED AIRCRAFT AND REMOTE CONTROLLED AIRCRAFT, ARE PROHIBITED WITHIN A 3 NMR UP TO AND INCLUDING 3000 FT AGL OF ANY STADIUM HAVING A SEATING CAPACITY OF 30,000 OR MORE PEOPLE WHERE EITHER A REGULAR OR POST SEASON MAJOR LEAGUE BASEBALL, NATIONAL FOOTBALL LEAGUE, OR NCAA DIVISION ONE FOOTBALL GAME IS OCCURRING. THIS NOTAM ALSO APPLIES TO NASCAR SPRINT CUP, INDY CAR, AND CHAMP SERIES RACES EXCLUDING QUALIFYING AND PRE-RACE EVENTS. FLIGHTS CONDUCTED FOR OPERATIONAL PURPOSES OF ANY EVENT, STADIUM OR VENUE AND BROADCAST COVERAGE FOR THE BROADCAST RIGHTS HOLDER ARE AUTHORIZED WITH AN APPROVED AIRSPACE WAIVER. AN FAA AIRSPACE WAIVER DOES NOT RELIEVE OPERATORS FROM OBTAINING ALL OTHER NECESSARY AUTHORIZATIONS AND COMPLYING WITH ALL APPLICABLE FEDERAL AVIATION REGULATIONS. THE RESTRICTIONS DESCRIBED ABOVE DO NOT APPLY TO THOSE AIRCRAFT AUTHORIZED BY AND IN CONTACT WITH ATC FOR OPERATIONAL OR SAFETY OF FLIGHT PURPOSES, DEPARTMENT OF DEFENSE, LAW ENFORCEMENT, AND AIR AMBULANCE FLIGHT OPERATIONS. ALL PREVIOUSLY ISSUED WAIVERS TO FDC NOTAM 9/5151 REMAIN VALID UNTIL THE SPECIFIED END DATE BUT NOT TO EXCEED 90 DAYS FOLLOWING THE EFFECTIVE DATE OF THIS NOTAM. INFORMATION ABOUT AIRSPACE WAIVER APPLICATIONS AND TSA SECURITY AUTHORIZATIONS CAN BE FOUND AT HTTP://WWW.TSA.GOV/STAKEHOLDERS/AIRSPACE-WAIVERS-0 OR BY CALLING TSA AT 571-227-2071. SUBMIT REQUESTS FOR FAA AIRSPACE WAIVERS AT HTTPS://WAIVERS.FAA.GOV

Federal Aviation Administration (FAA) Law Enforcement Guidance for Unauthorized UAS Operations, continued

11

Disney Theme Parks

FDC 4/XXXX ZZZ SECURITY SPECIAL NOTICE DISNEY WORLD THEME PARK ORLANDO FL THIS NOTAM REPLACES NOTAM 9/4985 TO REFLECT A TSA WEBSITE UPDATE AND ADDITIONAL INFORMATION CONCERNING AIRSPACE WAIVERS. FLIGHT RESTRICTIONS IN THIS NOTAM COMPLY WITH STATUTORY MANDATES DETAILED IN SECTION 352 OF PUBLIC LAW 108-7 AS AMENDED BY SECTION 521 OF PUBLIC LAW 108-199. PURSUANT TO 49 USC 40103(B), THE FEDERAL AVIATION ADMINISTRATION (FAA) CLASSIFIES THE AIRSPACE DEFINED IN THIS NOTAM AS 'NATIONAL DEFENSE AIRSPACE'. ANY PERSON WHO KNOWINGLY OR WILLFULLY VIOLATES THE RULES PERTAINING TO OPERATIONS IN THIS AIRSPACE MAY BE SUBJECT TO CERTAIN CRIMINAL PENALTIES UNDER 49 USC 46307. PILOTS WHO DO NOT ADHERE TO THE FOLLOWING PROCEDURES MAY BE INTERCEPTED, DETAINED AND INTERVIEWED BY LAW ENFORCEMENT/SECURITY PERSONNEL. PURSUANT TO 14 CFR SECTION 99.7, SPECIAL SECURITY INSTRUCTIONS, ALL AIRCRAFT FLIGHT OPERATIONS TO INCLUDE UNMANNED AND REMOTE CONTROLLED AIRCRAFT ARE PROHIBITED WITHIN A 3 NMR OF 282445N/0813420W OR THE ORL238014.8 UP TO AND INCLUDING 3000 FT AGL. THE RESTRICTIONS DO NOT APPLY TO THOSE AIRCRAFT AUTHORIZED BY AND IN CONTACT WITH ATC FOR OPERATIONAL OR SAFETY OF FLIGHT PURPOSES, AND DEPARTMENT OF DEFENSE, LAW ENFORCEMENT, AND AIR AMBULANCE FLIGHT OPERATIONS. FLIGHTS CONDUCTED FOR OPERATIONAL PURPOSES OF ANY DISNEY WORLD EVENT AND VENUE ARE AUTHORIZED WITH AN APPROVED WAIVER. AN FAA AIRSPACE WAIVER DOES NOT RELIEVE OPERATORS FROM OBTAINING ALL OTHER NECESSARY AUTHORIZATIONS AND COMPLYING WITH ALL APPLICABLE FEDERAL AVIATION REGULATIONS. ALL PREVIOUSLY ISSUED WAIVERS TO FDC NOTAM 4/4985 REMAIN VALID UNTIL THE SPECIFIED END DATE BUT NOT TO EXCEED 90 DAYS FOLLOWING THE EFFECTIVE DATE OF THIS NOTAM. INFORMATION ABOUT AIRSPACE WAIVER APPLICATIONS AND TSA SECURITY AUTHORIZATIONS CAN BE FOUND AT HTTP://WWW.TSA.GOV/STAKEHOLDERS/AIRSPACE-WAIVERS-0 OR BY CALLING TSA AT 571-227-2071. SUBMIT REQUESTS FOR FAA AIRSPACE WAIVERS AT HTTPS://WAIVERS.FAA.GOV

Attachment B.

Facility	States	Office	EMail
Western ROC	AK, AZ, CA, CO, HI, ID, MT, NV, OR, UT, WA and WY	425-227-1999	9-ANM-ROC@faa.gov
Central ROC	AR, IA, IL, IN, KS, LA, MI, MN, MO, ND, NE, NM, OH, OK, SD, TX and WI	817-222-5006	9-asw-operation-center@faa.gov
Southern ROC	AL, FL, GA, KY, MS, NC, PR, SC, TN and VI	404-305-5180	9-ASO-ROC@faa.gov
Eastern ROC	DC, DE, MD, NJ, NY, PA, VA and WV	718-553-3100	7-AEA-ROC@faa.gov
New England ROC	CT, MA, ME, NH, RI and VT	404-305-5156	7-ANE-OPSCTR@faa.gov
Washington WOC		202-267-3333	9-awa-ash-woc@faa.gov

APPENDIX 10

Sample Privacy Impact Assessment

Appendix A—Privacy Impact Assessment Template

Instructions for Completing the Privacy Impact Assessment—PIA Template Column Headings

The following information is provided to assist individuals in performing the PIA.

Template Section—PIA questions are grouped into sections of related policy concepts that mirror the framework of the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template), used to draft the entity privacy policy. Structuring the questions in this format prepares the practitioner performing the PIA for the next step, applying this information to the privacy policy.

PIA Questions—Pose questions for response or action.

Suggested Respondent(s)—General list of individuals (or roles) within the entity who are recommended to answer or contribute to the answer to the particular question. Other appropriate positions may be added or substituted as needed.

Entity Administrator: The chief executive officer or chief operations officer of the agency or organization. This could also be a department or division head over a particular organizational unit responsible for data collected and shared via an information exchange.

System Administrator: The chief information officer or other senior official responsible for overseeing the overall IT functions of an agency or organization.

Data Privacy Officer/Legal Counsel: The agency or organization privacy officer or attorney responsible for ensuring that the entity complies with all relevant privacy laws and policies. This should be the person who acts as the senior policy advisor on overall privacy policy, including legislative language, regulations, and other nonregulatory guidance related to or including privacy, confidentiality, or data security.

Technical/Systems Security Staff: The agency or organization staff person(s) responsible for implementing the technical enforcement of all relevant privacy and security policies (e.g., user authentication, access control, audit logs, firewalls, encryption).

Answer—The respondent(s) respond(s) to each question, as appropriate:

- Yes – Fully meets requirement
- No – Does not meet requirement
- Incomplete – Partially meets requirement
- N/A – Does not apply

Assessment of Risk—Make a judgment as to the likelihood, severity, and risk tolerance level of the privacy risk.[6] Recommended guidelines:

Likelihood that risk will occur

Remote: The risk probably will not occur because the risk would be difficult to realize, or there are solid means in place to limit the risk appropriately.

Possible: The risk has a chance of occurring, but it may be difficult or there are policies or procedures in place to help avoid the risk.

Likely: Because of conditions and capabilities, the risk is likely to occur.

Severity of identified risk

Low: The risk is manageable through planning and action, and the impacts generally are minimal.

Medium: The risk will be mitigated through planning and action. If it occurs, it will still have some impact on more important areas of concern.

High: The risk will have serious impacts; without extensive planning and action, its consequences would be severe.

Your tolerance for that risk

Avoidance: Avoidance is often used for risks that have the capacity for negative impact but have little known recourse. In privacy projects, a decision to avoid risks often means a decision not to let your agency put itself in a situation wherein it could incur the risk. Therefore, your decision would also be to avoid the cause of the risk.

Assume: The decision to assume a risk means accepting the risk as is and not implementing any policies or procedures to lessen it. This is often the decision in cases where the risk is so minimal and of such limited impact, should it occur, that the cost of implementing a mechanism to minimize or reduce it would be far greater than the agency's concern.

6 For more about risk assessment, see *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*, prepared by SEARCH, The National Consortium for Justice Information and Statistics, and published by the Office of Community Oriented Policing Services, U.S. Department of Justice. Available at www.search.org/files/pdf/ITSecTechGuide.pdf.

Sample Privacy Impact Assessment, continued

Mitigate: This is the most common decision to make for identified risks: to implement policies, procedures, and other controls to limit the risk to an acceptable level.

Transfer: Transfer the responsibility for a system or the risk itself to another party that can better accept and deal with the risk and/or that has the resources necessary to properly mitigate the risk.

- In the Corrective Action/Remediation column, record the corrective action or recommendation that your initiative will take to mitigate the identified risk.
- In the Assessment of Risk column, record the priority level of the risk: either 1 (high priority), 2 (moderate priority), or 3 (lowest priority).

Corrective Action/Remediation/Location—If the answer to the PIA question is "No" or "Incomplete," then respond in the Corrective Action/Remediation column as to what steps will be taken to respond to this requirement and who will be responsible for taking the necessary action(s).

If the answer to the PIA question is "Yes," then respond in the Corrective Action/Remediation column as to where the necessary information can be located to be included or referenced in the entity's privacy, civil rights, and civil liberties policy.

In the original document, page 16 is blank. It has been removed from these guidelines.

PIA Cover Page

Information Sharing System or Exchange(s) Assessed:	
System Names:	
Purpose:	
Assessment Date(s):	
Organizations/Entities Involved:	Assessors (Entity Representatives):
Project Manager:	
Final PIA Submitted to:	
Date Submitted:	
Approved by:	
Approval Date:	

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
A. Purpose Specification	1. Is there a written mission statement for the entity?	Entity Administrator
	2. Is there a written purpose statement for collecting personally identifiable information (PII)? Include all types.	Entity Administrator Data Privacy Officer/ Legal Counsel
	3. Does the entity's mission statement support the purpose for collecting PII?	Entity Administrator Data Privacy Officer/ Legal Counsel
B. Policy Applicability and Legal Compliance	1. Does the entity have legal authority for collecting, creating, storing, accessing, receiving, and sharing or viewing data? If so, include citation(s), if applicable.	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Will all individuals with physical or logical access to the entity information be subject to the privacy policy?	System Administrator OR Data Privacy Officer/ Legal Counsel
	3. How does the entity plan to provide the privacy policy to personnel, participating users, and individual users (for example, in print, online)?	System Administrator
	4. Will the entity require all individuals with physical or logical access to acknowledge receipt of the policy and agree to comply with the policy? (In writing or online?)	System Administrator
	5. Will the entity require that individuals with physical or logical access and information-originating and user agencies be in compliance with all applicable constitutional and statutory laws protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of information? Note: These laws, statutes, and regulations will be cited in the privacy policy.	System Administrator OR Data Privacy Officer/ Legal Counsel
	6. Is a privacy notice required by law before data is collected, where appropriate (usually limited to health records)?	System Administrator OR Data Privacy Officer/ Legal Counsel

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
C. Governance and Oversight	1. Is primary responsibility for the entity's overall operation—including the information systems, information collection and retention procedures, coordination of personnel, and enforcement of the privacy policy—assigned to one or more individuals?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Will the entity designate and train a privacy officer to handle reported errors and violations and oversee the implementation of privacy protections?	System Administrator
	3. Will the entity assign responsibility for ensuring that enforcement procedures and sanctions for noncompliance with the privacy policy are adequate and enforced?	Entity Administrator
D. Information	1. Has the entity identified the information it will seek, collect, retain, share, disclose, or disseminate?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity apply labels to information based on legal or policy restrictions or information sensitivity to indicate to authorized users how to handle the information?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	3. Does the entity categorize information based on its type (for example, tips and leads, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress), usability, and quality?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	4. Does the entity require certain basic descriptive information to be associated with each record, data set, or system of records containing PII (for example, source, originating entity, collection date, and contact information)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	5. Is personal information obtained with the knowledge or consent of the data subject, if appropriate?	System Administrator

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
E. Acquiring and Receiving Information	1. Are there applicable state and federal constitutional provisions and statutes that govern or specify the techniques and methods the entity may employ when seeking and receiving information? Note: These laws, statutes, and regulations will be cited in the privacy policy.	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity (if operational, conducting investigations) adhere to a policy regarding the investigative techniques to be followed when acquiring information (for example, an intrusion-level statement)?	System Administrator OR Data Privacy Officer/Legal Counsel
	3. Do agencies that access your entity's information and/or share information with your entity ensure that they will adhere to applicable law and policy?	System Administrator OR Data Privacy Officer/Legal Counsel
	4. Does the entity contract with commercial databases and, if so, does the entity ensure that the commercial database entity is in legal compliance in its information-gathering techniques?	System Administrator OR Data Privacy Officer/Legal Counsel
F. Information Quality Assurance	1. Has the entity established procedures and processes to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects and maintains, including procedures for responding to alleged or suspected errors or deficiencies (for example, correction or destruction)?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity apply labels (or ensure that the originating agency has applied labels) to the information regarding its level of quality (for example, accurate, complete, current, verifiable, and reliable)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	3. Does the entity review the quality of the information it originates to identify data that may be inaccurate or incomplete?	System Administrator OR Data Privacy Officer/Legal Counsel
	4. When information that is received from or provided to another agency is determined to be inaccurate or incomplete, does the entity notify the originating or recipient agency?	System Administrator OR Data Privacy Officer/Legal Counsel

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
G. Collation and Analysis	1. Is there a policy stating the purpose for which information is analyzed and specifying who is authorized (position/title, credentials, etc.) to analyze information?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Has the entity defined what information can be analyzed?	System Administrator OR Data Privacy Officer/ Legal Counsel
H. Merging Records	1. Does the entity identify who is authorized (position/title, credentials, clearance level[s], etc.) to merge records?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	2. Does the entity define matching criteria for merging information from multiple records allegedly about the same individual (e.g., sufficient identifying information beyond "name")?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	3. If the criteria specified above are not met, does the entity have a procedure for partial matches? Note: If the agency or exchange does not merge records that have partial matches, the policy should state this.	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
I. Sharing and Disclosure	1. Does the entity assign credentialed role-based levels of access for authorized users (for example, class of access and permissions to view, add, change, delete, or print)?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	2. Has the entity defined the conditions and credentials for access to and disclosure of records within the entity or in other governmental entities (for example, for law enforcement, public protection, public prosecution, public health, or justice purposes)?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	3. Are participating agencies that access information from your entity required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure laws applicable to the originating agency?	System Administrator OR Data Privacy Officer/ Legal Counsel
	4. Has the entity identified those laws or policies that specify when a record can be disclosed to a member of the public?	System Administrator OR Data Privacy Officer/ Legal Counsel
	5. Does the entity maintain an audit trail to document access to and disclosure of information retained by the entity (e.g., dissemination logs)?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	6. If release of information can be made only under exigent circumstances, are those circumstances described?	System Administrator OR Data Privacy Officer/ Legal Counsel
	7. Does the entity adhere to laws or policies for confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information?	System Administrator OR Data Privacy Officer/ Legal Counsel

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
J. Redress **J.1 Disclosure**	**Disclosure** 1. If required by law or policy, has the entity established procedures for disclosing information to an individual about whom information has been gathered (for example, proof of identity, fingerprints)?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Are there conditions under which an entity will not disclose information to an individual about whom information has been gathered? Note: The privacy policy will cite applicable legal authority for each stated basis for denial.	System Administrator OR Data Privacy Officer/ Legal Counsel
	3. If the entity did not originate the information and does not have the right to disclose it, are there circumstances in which the entity will either refer the individual to the agency originating the information or notify the originating agency of the request?	System Administrator OR Data Privacy Officer/ Legal Counsel
J.2. Corrections	**Corrections** 1. Has the entity established procedures for handling individuals' requests for correction involving information the entity has disclosed and can change because it originated the information?	System Administrator OR Data Privacy Officer/ Legal Counsel
J.3 Appeals	**Appeals** 1. If requests for disclosure or corrections are denied, does the entity have established procedures for appeal?	System Administrator OR Data Privacy Officer/ Legal Counsel

Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities

28

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
K. Security Safeguards	1. Does the agency or exchange have a designated security officer?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	2. Does the entity have physical, procedural, and technical safeguards for ensuring the security of its data? Note: The privacy policy will describe how information will be protected from unauthorized access, modification, theft, or sabotage (whether internal or external) resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, and physical security measures.	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	3. Is information stored in a secure format and a secure environment?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	4. Does the entity utilize watch logs to maintain audit trails of requested and disseminated information, and do logs identify the user initiating the query?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	5. Does the entity have established procedures for adhering to data breach notification laws or policies?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
L. Information Retention and Destruction	1. Does the entity have a records retention and destruction policy (including methods for removing or destroying information)?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity have a review schedule for validating or purging information?	System Administrator OR Data Privacy Officer/Legal Counsel
	3. Will there be a periodic review of collected data to make sure they are still needed? If so, include the review schedule.	System Administrator

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

Sample Privacy Impact Assessment, continued

Template Section	PIA Questions	Suggested Respondent(s)
M. Accountability and Enforcement **M.1 Information System Transparency**	**Information System Transparency** 1. Does the entity have a point of contact (position/title) for handling inquiries or complaints?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Will the privacy policy be available on the entity's public Web site?	System Administrator OR Data Privacy Officer/ Legal Counsel
M.2 Accountability	**Accountability** 1. Are there procedures and practices the entity follows to enable evaluation of user compliance with system requirements and applicable law, as well as its privacy policy, when established?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	2. Is there an established mechanism for personnel to report errors and suspected or confirmed violations of policies related to protected information?	System Administrator OR Data Privacy Officer/ Legal Counsel
M.3 Enforcement	**Enforcement** 1. Has the entity established procedures for enforcement (sanctions) if an agency or authorized user is suspected of being or has been found to be in noncompliance with the laws and policies, including the entity's privacy policy, when established?	System Administrator OR Data Privacy Officer/ Legal Counsel
N. Training	1. Will the entity require any individual having physical or logical access to entity information to participate in training programs regarding the implementation of and adherence to the privacy policy?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Will the entity's privacy training program cover the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations?	System Administrator OR Data Privacy Officer/ Legal Counsel

	Answer (Yes, No, Incomplete, or N/A)	**Assessment of Risk**	**Corrective Action/ Remediation/Location**

APPENDIX 11

UAS Legal Memoranda

Overview of UAS/UAV Technology and Regulation; Analysis of Police Use of UAS/UAV Systems Under U.S. Constitution and Case Law

SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Overview of UAS/UAV Technology and Regulation; Analysis of Police Use of UAS/UAV Systems Under U.S. Constitution and Case Law

TO: The Police Foundation and the U.S. Department of Justice – COPS Office

FROM: Anne T. McKenna, Esquire

RE: *Community Policing and UAS Guidelines to Enhance Community Trust*
2013-CK-WX-K002

SUBJECT: Domestic Law Enforcement's Use of UAS/UAV: A Legal Analysis of the U.S. Constitution, Statutory Law, and Case Law, and An Overview of UAS/UAV Technology

DATE: April 10, 2014; final edits July 31, 2014

SUMMARY OF LEGAL MEMORANDUM

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between the Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled, *Community Policing and UAS Guidelines to Enhance Community Trust* (the "COPS contract"). Pursuant to the COPS contract Task 1 (detailed description of work appended to the COPS contract) and as discussed with the Police Foundation's Grants Manager, Maria Valdovinos, this first memorandum ("Legal Memo: Police Use of UAVs and the Law") addresses the following:

I. An overview of Unmanned Aerial System (UAS) and Unmanned Aerial Vehicle (UAV) technology;

II. A brief review of Federal Aviation Administration (FAA) regulation of UAS/UAV technology;

III. Task 1's Line Item (1), which includes:

   A. an overview of the U.S. Constitution with a focus on the First and Fourth Amendment considerations in UAS usage

   B. an overview of the existing federal electronic surveillance statutory scheme and how it may govern and apply to UAS usage

IV. Task 1's Line Item (2), which includes research, review and analysis of all Supreme Court decisions and all major U.S. Courts of Appeal decisions that relate to use of various forms of electronic surveillance so that participants may grasp how courts are addressing government use of electronic surveillance and, to a much lesser extent, private industry use of electronic surveillance.

V. Conclusions

UAS Legal Memoranda, continued

SUBJECT INTRODUCTION

Advancements in electronic surveillance technologies in general and UAS/UAV technology in particular, now enable *domestic law enforcement* (collectively referred to as "police") to survey remotely public or open spaces, monitor traffic and air quality, conduct search and rescue missions, identify individuals in open spaces, etc., in non-intrusive and cost-efficient means. Current technology permits UAVs to be outfitted at a relatively low cost with high-powered cameras, thermal imaging devices, license plate readers, and laser radar.[1]

For the most part, however, the legality of police use of such evolving technologies in general and UAS/UAVs in particular has not heretofore been considered by courts. Police want to protect the public and to gather admissible evidence as thoroughly and efficiently as possible; it is fair to say that proper use of UAS/UAV technology would permit just that. But the Supreme Court's hodge-podge of electronic surveillance-related decisions and its openly acknowledged difficulty[2] in applying the framework of existing Fourth Amendment jurisprudence to advancing technologies adversely hampers officers' efforts to understand whether usage of these emerging technologies is permissible under the Fourth Amendment and its state equivalents.

In this memorandum, we attempt to address this conundrum and we provide a framework of analysis to assist police and the communities by whom they have been entrusted with safekeeping.

[1] Congressional Research Service Report, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses,* Thompson, Richard M., www.crs.gov (April 3, 2013).
[2] *See e.g., United States v. Jones*, 132 S.Ct. 945 (2012).

I. THE TECHNOLOGY: AN OVERVIEW OF UNMANNED AERIAL SYSTEMS (UAS) AND UNMANNED AERIAL VEHICLES (UAVs)

An UAV[3] is only one part of an UAS; the term UAS refers to the entire system, which includes the UAV, the digital network and electronic devices used to operate the UAV and the surveillance systems with which the UAV is equipped, as well as the personnel on the ground operating the UAV and operating the surveillance systems employed on the UAV. [4]

UAVs fly at slower paces and for longer intervals than their manned counterparts. They can fly autonomously, controlled by manned ground stations, or on a pre-programmed path below, in, or above piloted aircraft zones.[5] Current UAS models are incredibly diverse in size, function, and payload. They are generally categorized by size. Most commonly used for reconnaissance, surveillance, and inspection, small UASs weigh under fifty-five pounds (and can weigh as little as nineteen grams),[6] generally fly no higher than 400 feet above ground, and can remain airborne for several hours.[7] Larger UASs weigh more than fifty-five pounds, are capable of flying up to or above 60,000 feet, and can often remain airborne for days. They are most commonly used for data gathering, surveillance, and communications relay.[8]

Advancing technologies have enabled the UAV portion of an UAS to easily and cost-effectively be equipped with various electronic surveillance devices. We next briefly overview the specific and generally available forms of electronic surveillance that are available for use on the UAV portion of an UAS.

A. UAV Surveillance Capabilities: An Overview

Current technology permits UAVs to be outfitted at a relatively low cost with a variety of surveillance tools or payloads. The following electronic surveillance technologies can be employed via UAVs:

---

[3] UAVs come in a wide range of shapes and sizes. At the larger end of the spectrum is the Global Hawk used by the U.S. military: it is as large and nearly as fast as a business jet. At the smaller end, there are UAVs small enough to fit in a backpack or even the palm of a hand. For instance, the video-capable Nano Hummingbird, developed by California-based AeroVironment, weighs only two-thirds of an ounce. OBSERVATIONS FROM ABOVE: UNMANNED AIRCRAFT SYSTEMS AND PRIVACY**,** John Villasenor, 36 Harv. J.L. & Pub. Pol'y 457 (Spring, 2013).

[4] Congressional Research Service Report, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses,* Thompson, Richard M., www.crs.gov (Sept. 2012).

[5] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination,* Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)

[6] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)

[7] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination,* Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)

[8] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination,* Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)

UAS Legal Memoranda, continued

1. Optical devices:[9]

    a. High resolution visible light imaging (cameras with still photography and video capacity)
    b. Optically enhanced imaging—Night vision/FLIR
    c. Infrared sensors
    d. Electro-optical imagers[10]
    e. License Plate Readers[11]

2. Ultraviolet imaging

3. Synthetic aperture radar

4. Acoustical devices—"Listening In"[12]

5. Tracking devices

6. Thermal Imaging

7. Biometric identification systems: i.e., software and imaging capable of remote identification of individuals from a distance via biometrics, including face recognition, potential use of gait analysis, etc.[13]

8. Olfactory: Bio-surveillance systems[14] or "electronic noses"[15]

9. Weapons systems[16]

---

[9] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013)
[10] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination,* Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)
[11] *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Jenkins, Ben, 102 Ky. L.J. 161 (2014)
[12] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013).
[13] Biometrics are discussed in more depth below. For a lengthier discussion of potential biometric identification systems, see *Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd Ed.*, Chapter 31—Biometrics, Fishman & McKenna, (West/Thompson 2013).
[14] Biosurveillance systems, with sensors to detect radiation levels and chemicals in the atmosphere, enable situational awareness that may prove critical in the event of chemical or nuclear accident or in the event of a terrorist attack with weapons of mass destruction.
[15] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013)
[16] As noted, the International Association of Chiefs of Police (IACP) in its August 2012 *Recommended Guidelines for the use of Unmanned Aircraft* strongly discourages use of any weapons systems on a UAV.

With respect to weapons systems, The International Association of Chiefs of Police (IACP) in its August 2012 *Recommended Guidelines for the Use of Unmanned Aircraft* strongly discourages use of any weapons systems on an UAV. Key intelligence officials, including the U.S. President, have openly acknowledged that U.S. military operations involving UAS utilize UAVs that are equipped with weapons systems and that such military UAVs are used to conduct targeted strikes of enemy combatants and enemy targets.[17] Use of such military UASs/UAVs by domestic law enforcement would raise clear strong constitutional concerns and violate the *Posse Comitatus* Act, 18 U.S.C. § 1385, which prohibits use of military forces and equipment in domestic law enforcement.[18]

The use of UAVs equipped with weapons systems by police is strongly discouraged by the IACP as such use would likely generate strong public outcry and, in turn, legislative backlash against any type of police use of UAVs. Thus, our analysis of legal issues surrounding police use of UAS does not address police use of UAVs equipped with weapons systems other than to state preliminarily that it is undersigned counsel's legal opinion that police use of UAVs equipped with weapons systems and actual use of such weapons systems is illegal.

B. UAV Applications: Current Use and Potential Use of Surveillance Technologies

UAVs have already been successfully used domestically in search and rescue missions, surveillance during police standoffs, and border control.[19] The Customs and Border Protection Agency has been employing UAVs since 2005 to monitor illegal border crossings and drug trafficking.[20] Some police departments have begun using drones to increase security at large sporting events, assist in crime prevention, and survey private property.[21] NASA and NOAA have both used UAVs for scientific research, data collection, and environmental monitoring. [22] Other current uses by public entities include "law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training, and other government operational missions."[23]

---

[17] See e.g., *Delays in Effort to Refocus C.I.A. From Drone War*, The New York Times, Sunday cover story, April 6, 2014.
[18] Use of Army and Air Force as *posse comitatus*, 18 U.S.C. 1385, provides:
Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.
[19] *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Jenkins, Ben, 102 Ky. L.J. 161 (2014)
[20] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)
[21] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)
[22] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)
[23] *Fact Sheet – Unmanned Aircraft System (UAS)*, FAA Press Release, Duqette, Alison, (January 6, 2014) http://www.faa.gov/about/initiatives/uas/

UAS Legal Memoranda, continued

The FAA's plan to rapidly integrate UASs into the national airspace, discussed in more detail in Section II below, is causing an explosion in the technology and application of UAVs. Possible applications include the detection and observation of forest fires, surveying real estate development, monitoring hostage situations, and observation of oil pipelines.[24]

A brief discussion of the more commonly available electronic surveillance devices capable of use on UAVs is warranted.

GPS Tracking[25]

GPS stands for Global Positioning System; GPS devices are commercially available and readily affordable.[26] Typically, when one refers to "GPS" he or she is actually contemplating a GPS receiver.[27] The Global Positioning System is actually a constellation of twenty-seven Earth-orbiting satellites.[28]

In simplistic terms, the GPS receiver, which is the actual, electronic tracking device attached or used, locates no less than four of these orbiting satellites and computes the distance between itself and each satellite by analyzing high-frequency, low-power radio signals from the GPS satellites.[29] Using a mathematical principle known as trilateration, the GPS receiver uses these combined calculations to determine its own location.[30]

GPS reveals far more than a traditional electronic tracking device; a standard GPS receiver provides not only a particular location, but it can also, in real time, trace the person or thing's path, movement, and speed of movement.[31] GPS devices also maintain historical data recording the person or object's movements.[32] If a GPS receiver is left in "on" mode, it stays "in constant communication with GPS satellites."[33]

Thus, GPS can serve both passive tracking purposes (to locate a person or an object) as well as real-time tracking purposes (to track the real-time movement of a person or object as it is

---

[24] *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Jenkins, Ben, 102 Ky. L.J. 161 (2014)
[25] Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE TOOMEY MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters, 4th ed. 2012).
[26] GPS devices are available for less than $100. For that amount of money, a consumer can purchase a pocket-sized or smaller gadget that discerns your exact location on Earth at any moment. Marshall Brain & Tom Harris, *How GPS Receivers Work*, HOWSTUFFWORKS (Aug. 1, 2013, 3:49 PM), http://electronics.howstuffworks.com/gps.htm.
[27] *Id*.
[28] Twenty-four of these satellites are in constant operation and three extra satellites are maintained in space in the event of failure with one of the other twenty-foursatellites. *Id*.
[29] *Id*.
[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] *Id*.

actually occurring).[34] This distinction is referred to as passive monitoring (which describes location-only purposes monitoring) and active monitoring (which is described as real-time monitoring).[35]

As utilized on UAVs, GPS tracking can both permit the UAV operator to locate the UAV in the event line of sight or loss of control occurs while operating the UAV[36] and enable a UAV to locate and track a device equipped with GPS, including a particular phone, vehicle equipped with GPS, or other electronic device.

For government purposes, the use of GPS devices and GPS evidence is generally governed by the same statutes and case law progeny as traditional electronic tracking devices (see Section III below).[37] However, federal tracking laws typically do not apply to private industry's use of GPS tracking technology.[38]

License Plate Readers

Automated license plate readers (ALPR) are standard issue on many police vehicles and most large cities and states routinely employ ALPR. Some ALPR are mounted and stationary, often at toll booths or tunnel entrances such as the I-95 Harbor tunnel and tollbooth in Baltimore, others are moved throughout an area by officers.

The case law generally provides strong support for the legality of plate readers, but the public does not seem to appreciate the scope of the data collected and how long the data is retained. When the public does learn this, there is often a privacy outcry.[39] Given the concurring opinions in *U.S. v. Jones,* which are discussed in detail below, it is unclear how the current Supreme Court would react to government fusion centers, where data from plate readers, CCTV, and other forms of open space surveillance are merged together to create a comprehensive database that would easily enable police to review a 24/7 history of a citizens' travels and activities. We address questions of UAV-obtained data and data retention in a separate legal memorandum per Task 1's Line Item (6).

Surveillance Cameras; CCTV; Body Cameras

---

[34] See, Fredericks v. Koehn, 2007 WL 2890466 (D. Colo. 2007), adhered to on reconsideration, 2008 WL 3833775 (D. Colo. 2008), for discussion of active and passive monitoring.
[35] *Id*.
[36] http://www.satnews.com/story.php?number=915693999
[37] THE SPY WHO GPS-TAGGED ME, www.slate.com/articles/technology/2012/11/gps_trackers_to_monitor_cheating_spouses_a_legal_gray_area_for_private_investigators.html (last visited Aug. 8, 2013) [pull source].
[38] *Id*.
[39] The Minneapolis plate reader scandal story demonstrates this.

UAS Legal Memoranda, continued

A discussion of the use of cameras in open spaces is beyond the scope of this memo. Suffice it to say, cameras—in many forms, shapes and sizes—are routinely employed in open spaces. Such surveillance is cost-effective, poses a deterrent to crime, and provides extremely valuable evidence.

Where the legal quandary arises is when cameras are capable of sound recording, and when cameras are connected to or merged and equipped with other identification systems, such as biometric identification software like face recognition, and connected to databases that provide comprehensive information about the subject and or individual being recorded. Google glass provides an illustrative example.

Thermal Imaging

The Supreme Court has spoken about the warrantless use of thermal imaging devices on homes and private properties: it is unlawful. But thermal imaging devices that record far more data than the device at issue in *Kyllo* are becoming commonplace. Thermal imaging-like devices that detect far more than a heat emission and thus outline will become readily available. Is use of such devices permissible? Should law enforcement be able to detect an individual's rising heart rate or blood pressure without the individual knowing?

Biosurveillance Systems

Biosurveillance systems, with sensors to detect radiation levels and chemicals in the atmosphere, enable situational awareness that may prove critical in the event of chemical or nuclear accident or in the event of a terrorist attack with weapons of mass destruction.[40]

These electronic noses have not yet faced any serious challenges in the courts.

Biometric Identification Systems[41]

"Biometrics" is a general term that is used interchangeably to describe a characteristic or a process.[42] As a *characteristic*, biometrics is defined as "a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition."[43]

---

[40] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013)
[41] Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE TOOMEY MCKENNA, WIRETAPPING AND EAVESDROPPING (Thomson Reuters, 4th ed. 2012).
[42] For a definition of "biometrics," developed by the National Science & Technology Council's (NTSC) 2006 Subcommittee on Biometrics, see *Biometrics Glossary*, BIOMETRICS.GOV, http://www.biometrics.gov/documents/glossary.pdf (last visited Aug. 8, 2013).
[43] *Id*.

As a *process*, biometrics is defined as "[a]utomated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics."[44]

In 1907, the Department of Justice (DOJ) established a Bureau of Criminal Identification, which was based upon fingerprints.[45] In 1924, the DOJ tasked the precursor of the Federal Bureau of Investigation (FBI) with creating a national identification and criminal history system.[46] This led to today's Criminal Justice Information Services (CJIS) of the FBI.[47] By the 1960s, the United States had created automated technology for the storage and comparison of prints.[48] Digitization in the 1980s and early 1990s further increased the ease and efficiency of finger prints as a biometric identifier, and by the end of the twentieth century, fingerprint identification had become the norm for governments around the world. [49]

In the 1990s, private industry and the United States Government earnestly invested in developing new biometric identification technologies.[50] The early 1990s saw the beginnings of face recognition software development, and in 1993, the Department of Defense initiated its Face Recognition Technology program.[51] In 1994, "[t]he first patent granted for automated iris recognition was issued."[52] In 1996, the United States Army implemented real-time video face identification.[53]

In 2000, the Defense Advanced Research Projects Agency (DARPA) initiated the Human Identification at a Distance Program.[54] "The goal [of this program] was to develop algorithms for identifying individuals up to 150 . . . meters away [by combining] face and gait recognition technologies".[55] The stated "purpose of [this] program was to provide early warning . . . for force protection . . . terrorism, and crime."[56]

---

[44] *Id*.
[45] NAT'L SCIENCE & TECH. COUNCIL, THE NATIONAL BIOMETRICS CHALLENGE 5 (2011), *available at* http://www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf.
[46] Kenneth R. Moses et al., *Chapter 6: Automated Fingerprint Identification System (AFIS)*, *in* NAT'L INST. OF JUSTICE, THE FINGERPRINT SOURCEBOOK 6-1, 6-4 (Alan McRoberts ed., 2011), https://ncjrs.gov/pdffiles1/nij/225320.pdf.
[47] NAT'L SCIENCE & TECH. COUNCIL, THE NAT'L BIOMETRICS CHALLENGE 5 (2011).
[48] Moses et al., *supra* note 86 at 6-1, 6-4.
[49] *Biometrics Glossary,* NSTC, (2006), http://www.biometrics.gov/Documents/BioHistory.pdf (last visited 7/23/2012).
[50] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN.L. REV. 407, 419 (2012).
[51] *Id*. at 423.
[52] *Id*. at 419 n. 39.
[53] *Id*. at 423.
[54] *Id*. at 423-24.
[55] *Id.* at 424.
[56] *Id*. This program is one of the first examples of transition to biometric identification via remote technology. *See* NAT'L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS 18 (Heather Rosenker & Megan Hirshey eds., 2008), *available at* www.biometrics.gov/documents/biometrics_in_Government_Post-9/11.pdf.

UAS Legal Memoranda, continued

The events of September 11, 2001 ushered in dramatic changes in the use of biometrics and in funding for advancements in biometric technology.[57] 9/11 also provided the impetus for homeland security-related legislation that, with little constitutional consideration, funded the development and implementation of biometric identification systems and authorized the collection (by both overt and covert means), retention, and sharing[58] of individual biometric data.[59] In describing the impact of 9/11 on government-conducted electronic surveillance, one commentator noted:

> In this process, there is a widening of surveillance, with a range of personal data being collected for the purposes of securitized immigration control and a wide range of government agencies (and not only immigration agencies) having access to such data, as well as a deepening of surveillance (via the collection of extremely sensitive categories of personal data, including biometrics) .. . . Great emphasis [is] placed on the widening and deepening of information collection and sharing (including . . . biometrics) from a variety of sources.[60]

The astonishingly rapid developments in biometric identification systems have revolutionized government, military and private industry's security systems and means of identification of persons.[61] The use of biometrics and emerging biometric technologies continues to alter and change the way persons are and can be identified and, in turn, the way persons can be tracked and subjected to surveillance.[62] For instance, the technological advances in the biometric identification system known as face or facial recognition and the corresponding relatively recent ability of government and private industry to surreptitiously collect, retain and access hundreds of millions of individuals' facial biometric data have coalesced to permit the almost immediate identification of individual "faces in a crowd and three-dimensional face recognition."[63] Government and private industry have developed a variety of handheld mobile devices that permit collection and wireless verification of identity via fingerprint biometrics, face biometrics and iris scanning.[64]

---

[57] *See id*. at 425.
[58] *Id*. at 427-28. As a result of post-9/11 legislative changes, this sharing of data amongst government agencies occurs both horizontally (between federal agencies) and vertically (between federal and state and local governments). *See id.* at 45.9-61.
[59] *See* Valsamis Mitsilegas, *Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, 19 IND. J. GLOBAL LEGAL STUD. 3, 12 (2012).
[60] *Id*. at12-13.
[61] *See* Donohue, *supra* note 90, at 410.
[62] *See id*. For instance, in Israel, a security technology firm partnered with an Israeli company, i-Mature, to create Age-Group Recognition (AGR) software that requires a computer user to submit to a scan of a finger bone to determine age prior to accessing certain websites. *See* Press Release, EMC Corporation, RSA Security and i-Mature Partner on Next-Generation Biometric Technology to Further Protect Children on the Internet (Feb. 7, 2005), http://www.rsa.com/press_release.aspx?id=5497.
[63] NAT'L SCI. & TECH. COUNCIL SUBCOM. ON BIOMETRIS & IDENTITY MGMT., *supra* note 54, at 12.
[64] *Id.* at 13.

Thus, low cost "biometric handheld devices now make it possible to obtain rapid identification virtually anywhere."[65] Most people seem unaware of how private industry uses biometrics to identify and track individuals' location, preferences and associates.[66]

II. FEDERAL AVIATION ADMINISTRATION'S REGULATION OF UASs

The Federal Aviation Administration (FAA), a division of the US Department of Transportation, authorized the first UAS usage in 1990.[67] The FAA is the primary regulatory agency of UAS usage, but their domain of regulation is safety, not privacy.[68] For this reason, there have been recent pushes to include the Department of Justice and the Department of Homeland Security in determining privacy regulations for the usage of UASs.

---

[65] *Id*.
[66] *Cf.* Lisa Vaas, *Apple's Siri Voiceprints Raise Privacy Concerns*, NAKED SECURITY, SOPHOS (June 28, 2012), http://nakedsecurity.sophos.com/2012/06/28/apples-siri-voiceprints-raise-privacy-concerns/ (IBM employees unaware of security risks from use of mobile device apps).
[67] *Fact Sheet – Unmanned Aircraft System (UAS)*, FAA Press Release, Duqette, Alison, (January 6, 2014) http://www.faa.gov/about/initiatives/uas/
[68] *Drones in the Homeland: A Potential Privacy Obstruction Under the Fourth Amendment and the Common Law Trespass Doctrine*, Oyegunle, Ajoke, 21 CommLaw Conspectus 365 (2013)

UAS Legal Memoranda, continued

A. Current FAA Regulations

The FAA Modernization and Reform Act of 2012, signed into law by President Obama on February 14th, 2012,[69] provides funding to the FAA and requires the FAA to achieve the safe integration of UASs into the national airspace by September 30, 2015. This would include the development of acceptable standards of operations and certification, licensing of operators, air traffic requirements, and designation of safe national airspace. The law also states that the FAA will make recommendations and projections on "the best methods to enhance the technologies and subsystems necessary to achieve the safe and routine operation of civil unmanned aircraft systems in the national airspace system." [70]

Some components of the law have garnered intense opposition. Under this legislation, the FAA is required to remove much of the bureaucratic red tape that hinders government agencies from receiving COAs quickly.[71] The FAA is also required to allow "'a government public safety agency' to operate any drone weighing 4.4 pounds or less as long as certain conditions are met (within line of sight, during the day, below four hundred feet in altitude, and only in safe categories of airspace)." [72]

The FAA allows for the usage of UASs in very controlled conditions. Depending on the type of UAV, most operations must occur under 55,000 feet of elevation, and most operations are currently not authorized to operate in Class B airspace, which "exists over major urban areas and contains the highest density of manned aircraft in the National Airspace System."[73]

Presently, there are two ways to obtain permission to legally operate an UAS within the national airspace system. Civil operators must obtain a Special Airworthiness Certificate in the Experimental Category (SAC-EC), which allow for the performance of "operations for research and development, market survey, and crew training." [74]

---

[69] *Drones in the Homeland: A Potential Privacy Obstruction Under the Fourth Amendment and the Common Law Trespass Doctrine*, Oyegunle, Ajoke, 21 CommLaw Conspectus 365 (2013)
[70] FAA Modernization and Reform Act of 2012, Pub L. No. 112-95
[71] *The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones*, Burow, Matthew L., 39 New Eng. J. on Crim. & Civ. Confinement 427 (Spring, 2013)
[72] *The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones*, Burow, Matthew L., 39 New Eng. J. on Crim. & Civ. Confinement 427 (Spring, 2013)
[73] *Fact Sheet – Unmanned Aircraft System (UAS)*, FAA Press Release, Duqette, Alison, (January 6, 2014) http://www.faa.gov/about/initiatives/uas/
[74] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)

Governmental agencies, including law enforcement, may attain a Certification of Waiver or Authorization (COA) in order to legally operate a UAS.[75] COAs may be filled out online, and the number of COAs being issued is rapidly increasing.[76] COAs impose certain requirements on those who obtain them.[77] According to the FAA's publications, these requirements include: 1. COAs should define the airspace in which the UAV is permitted to fly; 2. COAs must mandate coordination with air traffic control facilities; 3. COAs mandate UAV operation within eyesight of the operator when flown in public airspace; and 4. COAs may include special provisions relevant to the operation of the specific UAS.

B. FAA's UAS Test Sites

In a press release on December 30, 2013, the FAA announced their selection of six UAS research and test sites around the country, including the University of Alaska, State of Nevada, New York's Griffiss International Airport, North Dakota's Department of Commerce, Texas A&M University, and Virginia Polytechnic Institute and State University (VA Tech).[78] The goal of these test sites is to conduct research on "certification and operational requirements necessary to safely integrate UAS into the national airspace over the next several years."[79] The FAA will assist operators in setting up safe testing environments and ensuring the operators' adherence to strict safety standards.

Police should look to the data coming from these test sites and from the FAA studies into UAS usage as an ongoing source of information to assist in state and local law enforcement use of UASs and as a source of information for the public.

C. Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS): the FAA Roadmap

[75] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)
[76] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)
[77] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)
[78] *Press Release – FAA Selects Unmanned Aircraft Systems Research and Test Sites*, Duquette, Alison, (December 30th, 2013) http://www.faa.gov/about/initiatives/uas/
[79] *Press Release – FAA Selects Unmanned Aircraft Systems Research and Test Sites*, Duquette, Alison, (December 30th, 2013) http://www.faa.gov/about/initiatives/uas/

UAS Legal Memoranda, continued

In accordance with the FAA Modernization and Reform Act of 2012, the FAA published in December of 2013 a roadmap that outlines the actions and considerations the FAA will take in order to ensure the safe integration of UAS into the National Airspace System (NAS). The following list of regulations is directly from that publication, and pertains to all UASs integrated into the NAS—police departments wishing to utilize UASs should necessarily be familiar and in compliance with these FAA UAS regulations:[80]

1. UAS operators comply with existing, adapted, and/or new operating rules or procedures as a prerequisite for NAS integration.
2. Civil UAS operating in the NAS obtain an appropriate airworthiness certificate while public users retain their responsibility to determine airworthiness.
3. All UAS must file and fly an IFR flight plan.
4. All UAS are equipped with ADS-B (Out) and transponder with altitude-encoding capability. This requirement is independent of the FAA's rule-making for ADS-B (Out).
5. UAS meet performance and equipage requirements for the environment in which they are operating and adhere to the relevant procedures.
6. Each UAS has a flight crew appropriate to fulfill the operators' responsibilities, and includes a pilot-in-command (PIC). Each PIC controls only one UA.*
7. Autonomous operations are not permitted.** The PIC has full control, or override authority to assume control at all times during normal UAS operations.
8. Communications spectrum is available to support UAS operations.
9. No new classes or types of airspace are designated or created specifically for UAS operations.
10. FAA policy, guidelines, and automation support air traffic decision-makers on assigning priority for individual flights (or flight segments) and providing equitable access to airspace and air traffic services. Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap.
11. Air traffic separation minima in controlled airspace apply to UA.
12. ATC is responsible for separation services as required by airspace class and type of flight plan for both manned and unmanned aircraft.
13. The UAS PIC complies with all ATC instructions and uses standard phraseology per FAA Order (JO) 7110.65 and the Aeronautical Information Manual (AIM).
14. ATC has no direct link to the UA for flight control purposes.

III. ELECTRONIC SURVEILLANCE LAW

A. <u>The U.S. Constitution: The First Amendment and the Fourth Amendment</u>

[80] *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, US Department Transportation, Federal Aviation Administration. First Edition, 2013.

1. The Right to Privacy: Development of the Concept and U.S. Common Law[81]

The word "privacy" does not appear in the United States Constitution, [82]but in their seminal 1890 Harvard Law Review article, *The Right to Privacy*, Samuel Warren and Louis Brandeis framed our modern constitutional and common law concepts of privacy.[83] In large part due to Warren and Brandeis's article, the U.S. Constitution—despite missing the magic *privacy* word—is the cornerstone of modern privacy law.[84] Common law privacy concepts and the common law right to privacy have flowed therefrom and, as evidenced by the amount of civil ligation cases asserting invasion of privacy-based claims, the U.S. common law provides for a robust right to privacy.

There are some marked similarities between today's societal and legal privacy struggles and those of the 1890s. At the time Warren and Brandeis's article was published, American society was facing aggressive, sensationalistic press (the term "Yellow Journalism" was coined to describe private press activities of the time);[85] there was incredible growth in newspaper circulation rates[86] (which fueled the financial rewards reaped from more invasive, intrusive newsgathering activities);[87] and technological developments, including readily available and affordable photography devices (this era saw the mass market introduction of Kodak's small snap camera)[88] and recording devices,[89] which permitted individuals to be recorded and photographed at an unprecedented rate.[90] These factors—(1) legally unfettered gathering of personal data (2) by private industry for commercial gain (3) enabled through advanced technologies—combined to foster invasions of individual privacy on a scale heretofore unimaginable.[91] When boiled down to the aforementioned factors, which spurred Warren and Brandeis to write their article and advocate for a new legal right, connecting the dots further is unnecessary: the similarity of these privacy issues in 1890 and the privacy concerns surrounding police use of UAS is strikingly similar.

---

[81] Portions of this discussion of the origins of U.S. privacy have been excerpted from Anne T. McKenna's law review article, *Pass Parallel Privacy Standards or Privacy Perishes*, 66 Rutgers L. Rev. 1041 (2013)
[82] *See* U.S. CONST.; *see also* Mark Silverstein, Note, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 218 (1989).
[83] *See* Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).
[84] *See generally id.*
[85] JOSEPH W. CAMPBELL, YELLOW JOURNALISM: PUNCTURING THE MYTHS, DEFINING THE LEGACIES 33 (2001).
[86] James H. Barron, *Warren and Brandeis,* The Right to Privacy*, 4 HARV. L. REV. 193 (1890): Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875, 889-90 (1979).
[87] *See id*. at 891.
[88] History of Kodak Milestones, KODAK, www.kodak.com/ek/us/en/our_company/history_of_kodak/milestones_chronology/1878-1929.htm.
[89] *See* DAVID R. SPENCER, THE YELLOW JOURNALISM: THE PRESS AND AMERICA'S EMERGENCE AS WORLD POWER 54 (David Abrahamson, ed., 2007).
[90] *See, e.g.*, *id.* at 2-3.
[91] *See, e.g.*, Barron, *supra* note 16, at 889-91.

UAS Legal Memoranda, continued

In their introduction to *The Right to Privacy*, Warren and Brandeis considered the Anglo-American jurisprudence system that enables our law's developmental flexibility to keep abreast of social, political, and technological changes.[92] The authors then highlighted how—enabled by developments in technology—the sacred precincts of private and domestic life were being invaded in ways not previously possible.[93] Warren and Brandeis then asked whether existing laws in 1890 were capable of protecting the privacy of the individual.[94] After an analysis of available legal remedies,[95] the two conclude that, while some laws may hinder certain types of privacy invasion, *e.g.*, libel and slander, existing laws were too limited in stopping unwanted personal data gathering by private industry.[96]

Warren and Brandeis looked to the U.S. Constitution itself and found that individual rights preserved by the First Amendment and the Fourth Amendment implicitly reflected a strong and vigorous right to privacy from government surveillance.[97] While Warren and Brandeis's concerns were focused on a privacy right that could protect the individual from private actors as opposed to state actors, their analysis of the First and Fourth Amendments were prescient to the UAV debate.

By providing the factual stage and describing in detail the nature of injury caused by privacy invasions, Warren and Brandeis unequivocally demonstrate the societal need for a new right.[98] The two then persuasively explain how the right to privacy is both derived from and present throughout our common law and historical concepts of "an inviolate personality" and "the right to be let alone."[99] Pointing to privacy protections afforded by tort law, evidence, property rights, contract law, and criminal law, the two establish that the right to privacy is not a new concept but something carried throughout all of these sources of common law, constitutional law, and statutory law.[100] Warren and Brandeis frame what the scope of the right to privacy is, the remedies it should afford, and reject what criticisms they foresee to the recognition of the right to privacy.[101] Warren and Brandeis's proposed common law right to privacy was ultimately recognized and adopted by the United States Supreme Court and by state courts and state legislatures across the nation.[102]

---

[92] Warren & Brandeis, *supra* note 15, at 193-95.
[93] *See id.* at 195.
[94] *See id.* at 197.
[95] *See id.* at 197-207.
[96] *See id.* at 207.
[97] *See id.* at 198.
[98] *See id*. at 197-98.
[99] *See id*. at 193, 197-205.
[100] *See id*. at 197-214.
[101] *See id*. at 214-20.
[102] *See generally* Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623 (2002) (examining the legal impact and legacy of The Right to Privacy); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479 (1990) (tracing the development of privacy rights from The Right to Privacy).

2. The First Amendment

The First Amendment to the U.S. Constitution provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Critics of police use of UASs raise the point that such use potentially violates the First Amendment's guarantee of freedom of association because the ability of police to know one's location and travels at all times will have a chilling effect on the freedom of association and free expression. As discussed below, Justice Sotomayor articulated similar concerns, albeit it with respect to police use of a GPS tracking installed on a car rather than police tracking via UAVs, in her concurrence in the Supreme Court's 2012 decision in *U.S. v. Jones*.[103]

In contrast, other commentators note that private use of UAVs as a method of news gathering is a First Amendment right.[104]

The most effective way to address Justice Sotomayor's First Amendment concerns and the public's fear is ensuring that police adhere to clearly specified acceptable use practices for UAVs and clearly expressed data gathering and data retention practices for data gathered via UAVs. A routine UAV patrol that monitors traffic or borders or environmental conditions is very different than the use of a UAV to surreptitiously track a certain individual for an extended period of time without a warrant.

3. The Fourth Amendment

The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

---

[103] U.S. v. Jones, 132 S.Ct. 945, 956 (J. Sotomayor, concurring):

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).

[104] http://voxglobal.com/2014/02/privacy-policy-drones-and-the-first-amendment/, Walt Sharp, author, article posted 2/18/14 (site last visited 4/7/14).

UAS Legal Memoranda, continued

> describing the place to be searched, and the persons or things to be seized.[105]

The Fourth Amendment applies only to government search and seizure.[106] It does not apply to private industry or third party search and seizure.[107] Section III.C., below, sets forth the Supreme Court's Fourth Amendment jurisprudence, and the Court's development of the reasonable expectation of privacy test and the third-party doctrine.[108] It specifically considers the Court's more recent, technology-specific Fourth Amendment cases to illustrate the application of the Fourth Amendment, the reasonable expectation of privacy test, and the third-party doctrine to the use of UASs, including emerging surveillance technology and existing digital data collection practices and geolocation tracking.

B. The Federal Legislative Scheme[109]

This section of Legal Memo: Police Use of UAVs and the Law overviews the federal statutory scheme that specifically pertains to electronic surveillance of communications and tracking. It does not address UAS/UAV specific legislation, which is addressed separately by the Police Foundation working with the consultant, per Task 1's Line Items (3) and (4). Pending federal legislation is also briefly discussed.

1. Title III

In 1968, in response to considerable social and political activity on a variety of fronts, Congress enacted the Omnibus Crime Control and Safe Streets Act.[110] Title III of that Act regulates interception of communications by public officials and private persons. In general terms, the electronic surveillance statutory scheme developed by Congress is collectively referred to as Title III.

Congress enacted Title III with two primary goals in mind. First, it sought to safeguard the privacy of wire and oral communications[111]—electronic communications were added to the

---

[105] U.S. CONST. amend. IV.
[106] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[107] *See id.*
[108] *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) (discussing reasonable expectations of privacy test); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011) (discussing third-party doctrine).
[109] Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE TOOMEY MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters, 3rd Ed. 2012), which provides a much more extensive discussion of the federal electronic surveillance legislative scheme.
[110] P.L. No. 90-351, 82 Stat. 197, 211 (1968), codified at 18 U.S.C.A. §§ 2510 et seq.
[111] Pub. L. No. 90-351, § 801(b), 82 Stat. 211 to 212 (1968); Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2177. State v. Gilmore, 201 Wis. 2d 820, 549 N.W.2d 401 (1996) (citing CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters ed., 3rd ed. 2007).)

statute's coverage in 1986[112]—and, in particular, the privacy of innocent persons.[113] Thus, Title III forbids the interception of wire, oral or electronic communications by private persons unless the communication is intercepted by, or with the consent of, a participant, and significantly restricts the authority of law enforcement officials to intercept such communications. Second, it sought to provide law enforcement officials with a much-needed weapon in their fight against crime, particularly organized crime,[114] by empowering them to intercept such communications under carefully regulated circumstances. With regard to the latter goal, Congress endeavored to satisfy the procedural and substantive requirements previously enunciated by the Supreme Court, in *Berger v. New York*[115] and *Katz v. United States*,[116] as constitutional prerequisites to a valid interception-of-communication statute,[117] while defining "on a uniform basis"—applicable to state, as well as federal government—"the circumstances under which the interception of wire and oral communications [and, subsequently, electronic communications] may be authorized" by a judicially issued interception order.[118]

Title III is a detailed legislative scheme. It specifies who may authorize an investigator to apply for a court order, the information an application must contain, the findings a judge must make before issuing the order, how the order is to be executed, how recordings of intercepted conversations are to be secured, who must eventually receive notice that a phone or other communications facility was tapped or a location was bugged, among other details. The statute describes when information obtained from intercepted communications may be disclosed, identifies who may seek to suppress evidence and on what grounds, and sets forth an exclusionary rule. It also created a civil cause of action for those whose communications are unlawfully intercepted.

An in-depth analysis of the federal electronic surveillance legislative scheme is well beyond the scope of Legal Memo: Police Use of UAVs and the Law. For our purposes, however, there are components of this scheme to briefly consider because of the likelihood that electronic surveillance devices employed via UAVs may fall within the scope of the statutes. Specifically, in 1986, the Electronic Communications Privacy Act (ECPA) amended Title III's

---

[112] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 1:15 (Thomson Reuters ed., 3rd ed. 2007).

[113] Pub. L. No. 90-351, § 801(d), 82 Stat. 211 to 212 (1968), Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2177.

[114] Pub. L. No. 90-351, § 801(c), 82 Stat. 211 to 212 (1968) (legislative findings introducing Title III); Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2157, 2177.

[115] Berger v. State of N.Y., 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967).

[116] Katz v. U.S., 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

[117] Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2161 to 62.

[118] Pub. L. No. 90-351, § 801(b), 82 Stat. 211 to 212 (1968), Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2153, 2177.

UAS Legal Memoranda, continued

definition of "wire communication" to include "electronic" communications.[119] The broad definition of "electronic" communications brings a host of modern, Internet-based communications, within ECPA's purview. Because ECPA expanded the definition of communications protected from surveillance, police use of any electronic surveillance device on an UAV that would permit interception of protected forms of communication must comply with ECPA.

In terms of tracking devices, there are only two federal statutes that directly address the use of tracking devices, and these only apply to law enforcement.[120] The Pen/Trap Statute regulates the use of pen/trap devices,[121] and the Stored Communications Act (SCA) also regulates storage of and access to stored electronic communications.[122]

The ECPA's SCA authorizes government access to stored communications in the hands of third party providers.[123] The SCA categorizes different types of stored communications (information) and outlines what the government must do to obtain access to those different types of communications.[124] The protection afforded by the SCA to these different types of information is based upon the type of stored information sought, i.e. addressing or dialing information—which by system design is in the hands of the third party provider for routing purposes—is afforded the least protection), whereas "content" information—which refers to the actual substance of the communication (whether email or voice call)—is afforded the greatest protection from surveillance).[125]

The Communications Assistance for Law Enforcement Act (CALEA) forbids the communications service providers, such as Verizon or Sprint, from producing "any information that may disclose the physical location of the subscriber" when the provider is producing call identifying information pursuant to the Pen/Trap Statute.[126] Thus, CALEA specifically limits information that providers may produce to law enforcement pursuant to the Pen/Trap Statute.

While this complex federal legislative scheme regulates both private actors and government, it regulates private and government actors in different ways.[127] The scheme does not limit what personal information and geolocation data the private actor or provider may collect, but it limits what information the private actor may give the government in the absence of court order.

---

[119] 18 U.S.C. § 2510 (2006).
[120] *See id*.§ 3117; 47 U.S.C. § 1002 (2006).
[121] 18 U.S.C.§§ 3121-3127,
[122] *Id.* § 2703.
[123] 18 U.S.C.§§ 2701 *et seq*.
[124] *Id*.
[125] *Id.*
[126] 47 U.S.C.§ 1002(a)(2)(B).
[127] *Id*.

Depending upon the purpose for which UAV based electronic surveillance may be employed, it is likely that Title III and related tracking device legislation will govern usage.

Corresponding State Wiretapping Statutes

The majority of states have mini-wiretapping acts and in some cases, such as Maryland and California, the corresponding state legislation is greater in its privacy protections. Police in such jurisdictions are strongly urged to be familiar with state and local electronic surveillance legislation, particularly in jurisdictions where there are variants from federal law.

2. Pending Legislation

Federal Proposed or Pending Legislation

The following are recently proposed Congressional bills that, if enacted, will impact the use of UAVs and other electronic surveillance devices at a domestic law enforcement level:

a. *Preserving Freedom from Unwarranted Surveillance Act of 2012 (S. 3287, H.R. 5925).* Would require law enforcement to obtain a warrant before using drones for domestic surveillance.
b. *Preserving American Privacy Act of 2012 (H.R. 6199).* Would permit law enforcement to conduct drone surveillance pursuant to a warrant, but only in investigation of a felony.
c. Other pending legislation includes multiple proposed electronic tracking laws passed in response to *US v. Jones,* and growing privacy concerns over tracking via geolocation data.

State Proposed or Pending Legislation

According to the NCSL, forty-three states have introduced 96 bills and resolutions concerning UAVs and UASs. As noted above, six bills have been enacted and resolutions have been adopted in six states.[128]

IV. FEDERAL COURT DECISIONS: GUIDANCE FOR POLICE USE OF UASS

A. <u>Supreme Court Decisions</u>

While the United States Supreme Court has yet to specifically consider whether the domestic law enforcement's use of many advancing technologies, in general, and UAVs, in particular, raises constitutional concerns, there is a complex and long-standing Fourth Amendment jurisprudence that can be applied to the use of UAVs and electronic surveillance devices with which a UAV may be equipped. By considering and familiarizing themselves with

[128] www.ncsl.org/issues-reserach/justice/unmanned-aerial-vehicles.aspx

UAS Legal Memoranda, continued

the Court's prior Fourth Amendment rulings, police can ascertain what types of emerging electronic surveillance technologies may be legal.

The Fourth Amendment to the United States Constitution prohibits unreasonable search and seizure. For decades, the United States Supreme Court has considered the constitutionality of searches conducted with technology that enhances a human's own ability to see, follow, feel, hear or smell. The framework of this Fourth Amendment jurisprudence guides our discussion today, and the following layman-styled overview of that jurisprudence provides the necessary framework for police to gauge how such technologies may be appropriately used:

1. Katz v. United States (1967)—Listening Device in Public Phone Booth

In *Katz*,[129] the Court held that it violated the Fourth Amendment to attach a listening device to a public telephone booth. This reflected a significant development in the Court's Fourth Amendment rationale: the Court explicitly recognized that the Fourth Amendment protects people, not places. And Justice Harlan's Concurrence set the stage for a major development in our modern day concept of privacy, which is that one must have a reasonable expectation of privacy (RXP) for society and the law to recognize it and protect it.

The concept of RXP fundamentally changed privacy law, but technological advances have called the RXP analysis into question. When considering whether a person has an RXP in any given situation, courts consider this subjectively and objectively—so disclosure to a 3rd party takes on greater significance as policy and laws develop around how we protect privacy in our lives…so if you knowingly expose something to the public or voluntarily turn information over to someone else (a third party)…then you cannot be said to have a reasonable expectation of privacy.

Usage of UAVs in open spaces has not yet faced challenge in federal court, and for now, police may rely in good faith upon this RXP test.

2. Maryland v. Smith (1979) – Disclosure and the Third Party Doctrine

In *Smith v. Maryland*, 442 U.S. 735 (1979), the defendant had disclosed the phone numbers he dialed out to the telephone provider. The Court held that this voluntary disclosure to the telephone provider was third party disclosure, and thus it was no longer afforded them Fourth Amendment protection. If blindly applied to the Internet, *Smith v. Maryland*'s third party doctrine would result in the vast majority of our electronic information being unprotected by the Fourth Amendment.[130]

3. United States v. Knotts (1983)—Tracking Beeper

[129] Katz v. U.S., 389 U.S. 347 (1967)
[130] *See id*.

In *Knotts*,[131] the Court ruled that law enforcement did not violate the Fourth Amendment when, without a warrant, officers attached a tracking beeper to a container of chloroform. The beeper was placed in the container with the owner's consent prior to the defendant's taking possession of the container. The development in rationale is that a person travelling on a public thoroughfare has no RXP in his movements from one place to another.

This will be significant when a court considers the use of UAV enabled with a license plate reader to track an individual on a public roadway.

4. United States v. Karo (1984)—Tracking Beeper

In *Karo*,[132] the Court added a complicated nuisance: the Court ruled that installation of a tracking device without a warrant but with the consent of the original owner did not constitute a search—but—the Court held that once officers turned the tracking beeper on without a warrant, officers had conducted a search in violation of the Fourth Amendment.

5. Dow Chemical Co. v. United States (1986); California v. Ciraolo (1986) and Florida v. Riley (1989) —the Aerial Surveillance Photography Cases

In *Dow*,[133] the Court considered the Environmental Protection Administration's ("EPA") use of a commercial aerial photographer to photograph a Dow Chemical facility that Dow refused to allow the EPA to inspect. Claiming that the photographs might reveal valuable trade secrets that it had gone to considerable lengths to protect (particularly with regard to several open-air plants), Dow argued that the EPA's action constituted a search that violated the Fourth Amendment.[134]

Dow, like *Ciraolo*[135] and *Riley*[136]—two other Supreme Court cases involving the constitutionality of aerial surveillance—poses questions concerning the applicability of the Fourth Amendment to aerial surveillance. The cases differ, however, in two significant respects:

- First, unlike the naked-eye surveillance in *Ciraolo* (photos taken from a plane at 1000 feet of the fenced yard of a private residence) and *Riley* (photos taken from helicopter at 400 feet of the fenced yard of a private residence), the *Dow* surveillance was conducted with an aerial mapping camera that recorded on film far more than an observer in the

[131] 460 U.S. 276 (1983)
[132] United States v. Karo, 468 U.S. 705 (1984)
[133] Dow Chemical Co. v. U.S., 476 U.S. 227, 106 S. Ct. 1819, 90 L. Ed. 2d 226, 24 Env't. Rep. Cas. (BNA) 1385, 16 Envtl. L. Rep. 20679 (1986), Fishman and McKenna, Wiretapping and Eavesdropping § 30:13
[134] Fishman and McKenna, Wiretapping and Eavesdropping § 30:13
[135] In *Ciraolo*, 476 U.S. 207 (1986), the Supreme Court ruled that there was no Fourth Amendment violation when Officers flew over a private residence at 1000 feet and took photographs after receiving a tip about a marijuana grow operation.
[136] In Florida v. Riley, 488 U.S. 455 (1989), the Court again ruled that photographs taken from a helicopter at 400 feet over a private residence did not constitute a search.

UAS Legal Memoranda, continued

plane could have seen with the naked eye. Thus, the surveillance in *Dow* was far more revealing than that in *Ciraolo* and *Riley*.

- Second, while *Ciraolo* and *Riley* involved surveillance of a curtilage of a private home, *Dow* involved surveillance of a huge multi-building industrial complex.[5]

The Court in *Dow* focused most of its Fourth Amendment attention on the question of whether the Dow complex should be likened to residential curtilage or an open field. A five-to-four majority opinion written by Chief Justice Burger, concluded that "for purposes of aerial surveillance," the latter analogy is more apt, and rejected Dow's claim.

Under the *Dow* case, the question of whether an UAV is employed in public airspace versus non-public airspace will be critical in determining the constitutionality of the usage.

6. <u>NY v. Class (1986)—Exterior of Automobile</u>

In *Class*,[137] the Court held that the exterior of an automobile is necessarily thrust into the public eye, so there is no RXP in that exterior and to visually examine it without a warrant does not constitute a search.

This is significant for UAV use because it supports the position that what is visible to any person standing in public is not protected by the Fourth Amendment. This strongly supports the argument that use of a UAV to see people, objects and activities that are knowingly exposed to the public does not raise Fourth Amendment concerns. Thus, the use of UAVs to monitor traffic conditions, weather conditions, a suspect publically fleeing police, a border crossing, an open field, etc., is permissible.

7. <u>Kyllo v. United States (2001)—Thermal Imaging Devices</u>

Resolving a split in the Circuits, the Supreme Court in *Kyllo*[138] held that the warrantless use of a thermal imaging device on a private residence constituted a search that violated the right to privacy afforded by the U.S .Constitution. *Kyllo* reflects a development in the Court's modern day privacy policy rationale: despite advances in technology, the Court will protect Constitutional concepts of privacy.

But the dissent in *Kyllo* presciently argued that Justice Scalia's rule—"firm but bright line of privacy at the door of the home"—would become problematic and defunct when the thermal imaging technology at use in *Kyllo* became readily available to the general public. And now we are there: thermal imaging devices are cheap and readily available to the public.

[137] NY v. Class, 475 U.S. 106 (1986).
[138] Kyllo v. US, 533 U.S. 27 (2001)

Thermal imaging devices are commonly available for installation and use on UAVs. Thus, the prudent officer who needs to employ thermal imaging via an UAV will seek a warrant.

8. Illinois v. Caballes (2005)—Dog Sniff No. 1—a traffic stop

In *Caballes*,[139] the Court ruled that officers did not violate the Fourth Amendment when they used of a drug-sniffing canine during a routine traffic stop where the sniff search did unreasonably prolong the length of the stop.

9. City of Ontario v. Quon (2010)—Text Messages

Having personally attended oral arguments in *Quon*,[140] I witnessed firsthand the Justices' discomfort with, understanding of, and difficulty in applying traditional RXP concepts to technological advances.[141] The Court in *Quon* determined that a SWAT team officer's superiors did not violate the Fourth Amendment when the supervising officer reviewed Officer Quon's text messaging to determine whether data overages were a problem under the City's data contract with a wireless provider. In the process of that pager audit, the supervisor saw Quon's lurid sexual text messages. But the Court ruled purely on the reasonableness of the pager audit, explicitly refusing to consider "far-reaching issues" it raised on the grounds that modern technology and its role in society was still evolving.[142]

The Court's struggle with understanding the capabilities of advancing technologies was uncomfortably on display during oral arguments in *City of Ontario v. Quon*.[143]. In *Quon*, the Court considered whether Special Weapons and Swat Team ("SWAT") members have an expectation of privacy in personal text messages sent on pagers issued by the city that employs them.[144] The Justices' struggle with the pager technology involved in the case was awkward. Chief Justice Roberts asked what would happen if a text message was sent to an officer at the same time he was sending a text to someone else,[145] at which point Justice Kennedy asked whether the officer in that situation would receive "a voice mail saying that your call is very important to us; we'll get back to you."[146] Both Justices Roberts and Scalia were openly grappling with the concept of a service provider when they stated they did not know that text

[139] Illinois v. Caballes, 543 U.S. 405 (2005)
[140] City of Ontario v. Quon, 130 S.Ct. 2619 (2010).
[141] The reporters' galley actually laughed out loud when one of the Justices asked during oral argument if someone could somehow print out and see Quon's text pages from his SWAT team pager.
[142] Justice Scalia harshly criticized the Court's rationale in his concurrence. He considered the majority opinion "vague" and charged his fellow justices with "disregard of duty" for their refusal to address the Fourth Amendment issues. A month after *Quon* was handed down, an appellate panel in a Georgia case similarly criticized it for "a marked lack of clarity" as it narrowed an earlier ruling to remove a finding that there was no expectation of privacy in the contents of email.
[143] *See* Transcript of Oral Argument at 44, *Quon*, 130 S. Ct. 2619 (No. 08-1332).
[144] *See Quon*, 130 S. Ct. at 2627.
[145] Transcript of Oral Argument at 44, (Roberts, C.J) ("What happens, just out of curiosity, if you're – he is ont the pager and sending a message and they're trying to reach for him, you know, a SWAT team crisis? Does he – does the one kind of trump the other, or do they get a busy signal?")
[146] *Id.*

UAS Legal Memoranda, continued

messages are sent to a service provider before going to the intended receiver.[147] Such questions are particularly concerning because the Justices lack an understanding that, by design, today's technology discloses all of one's personal information to third parties.[148] Accordingly, under the third party doctrine in *Smith v. Maryland* in 1979, the vast majority of our electronic information would be unprotected.[149]

10. United States v. Jones (2012)—Warrantless Use of a Tracking Device

In 2012, the Court unanimously affirmed a 2010 decision from the United States Court of Appeals for the D.C. Circuit wherein the lower appellate court had ruled that law enforcement's warrantless attachment of a GPS device to a car and subsequent warrantless use of that GPS device to track defendant Jones for a period of 28 days constituted an unlawful search in violation of the Fourth Amendment. Although unanimous in their decision to affirm the D.C. Circuit, the Justices arrived at their unanimous holding through two sharply and evenly divided camps of rationale, with Justice Sotomayor striking out on her own.

For purposes of analysis, the *Jones* decision reflects a hard step backwards in considering law enforcement's use of advanced tracking in open spaces. Why? Because in this case, the Supreme Court took on law enforcement's warrantless use of GPS tracking devices.[150] The majority opinion based its holding on the act of trespass that occurred when police physically attached the GPS device to the suspect's vehicle.[151]

The *United States v. Jones* decision is remarkable in many respects, but for purposes of our discussion, there are three notable aspects of the decision. First, given earlier beeper and GPS-based location tracking decisions, it is striking that all nine Justices unanimously agreed that the warrantless installation of a GPS tracking device on a suspect's car and subsequent tracking for twenty-eight days constituted an impermissible search.[152] Second, although the

---

[147] *See id*. at 48-49 ("MR DAMMEIER: Well, they --they expect that some company, I'm sure, is going to have to be processing the delivery of this message. And --
CHIEF JUSTICE ROBERTS: Well, I didn't --I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing. (Laughter).
MR. DAMMEIER: Well --
JUSTICE SCALIA: You mean it doesn't go right to the other thing? (Laughter)."),
[148] *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[149] *See id*.
[150] United States v. Jones, 132 S. Ct. 945 (2012).
[151] *See id*. at 953. There were three opinions issued with the ruling: Justice Scalia authored the majority opinion, which was joined by Justices Roberts, Kennedy, Thomas, and Sotomayor; Justice Sotomayor also filed her own concurring opinion; and Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, filed a concurring opinion as well.
[152] For example in United States v. Knotts, the Court held that the use of a beeper to track Knotts's location was constitutional because a person does not have a reasonable expectation of privacy on public thoroughfares because one's movements are exposed to the public. 460 U.S. 276, 281-82 (1983). Additionally, police use of the beeper to supplement their visual surveillance did not result in a Fourth Amendment violation. *Id*. at 282. Rather, the Court stated: "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." *Id*.

Justices were unanimous in their conclusion, the differences in the Justices rationales was stunning.[153] And third, the Justices' open struggle with certain issues reflects the increasing quagmire at the intersection of advancing technologies, privacy and reasonable expectations of privacy.[154]

In *Jones*, while the majority held the use of a GPS device to conduct prolonged surveillance was unconstitutional, it did so only because it found the police's physical act of attaching a GPS device to Jones's car was a trespass on Jones's property.[155] As Justice Sotomayor notes in her concurring opinion, a search occurs "at a minimum" where the government physically intrudes on a constitutionally protected area.[156] Her concurrence and Justice Alito's concurrence acknowledge very problematic limitations of the Court's decisions: advanced capabilities of new technologies enable the collection of vast amounts of data without a physical trespass.[157]

11. <u>Florida v. Jardines (2013)—Dog Sniff No. 2—on the Front Porch</u>

In *Jardines*,[158] the Court surprised some legal scholars: it ruled that a dog sniff at the front door of a house where officers suspected drugs were being grown constituted a Fourth Amendment search. Justice Scalia, who wrote the majority opinion, decided it purely on property grounds. While at first blush, the decision reflects a problem for UAV usage, the rationale is purely non-technology based. Justice Kagan's concurrence provides more useful guidance for our analysis of electronic surveillance devices: she describes the dog as a form of enhanced technology—a "super sensitive instrument, which the police deployed to detect things inside that they could not have perceived unassisted."

In *Florida v. Jardines*, police took a drug sniffing dog to the front porch of Jardines's home where police suspected Jardines was growing marijuana.[159] The dog tracked a scent he had been trained to detect and eventually sat, indicating that he had discovered the odor's

---

[153] Compare *Jones*, 132 S. Ct. at 949 (Scalia, J.) ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted."), *with id*. at 955 (Stomayor, J., concurring) ("In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion of property, the majority opinion's trespassory test may provide little guidance."), *with id*. at 958 (Alito, J., concurring) ("I would analyzing the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long term monitoring of the movements of the vehicle he drove.").
[154] *See id*.
[155] *Jones*, 132 S. Ct. at949,
[156] *Id*.at 954 (Sotomayor, J., concurring).
[157] *Id*. at 959 (Alito, J., concurring) (("'[T]he search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.'" (quoting Goldman v. United States, 316 U.S. 129, 135 (1942))).
[158] Florida v. Jardines, 569 U.S. ___ (2013).
[159] Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).

UAS Legal Memoranda, continued

strongest point.[160] The Court considered whether using a drug sniffing dog on Jardines's porch to investigate the contents of his home constituted a search.[161]

In a 5-4 decision, Justice Scalia and the majority held that the use of the dog on the front porch constituted a search within the meaning of the Fourth Amendment because the police learned what they learned only by physically intruding onto Jardines's property.[162] The majority did not consider the *Katz* analysis or the use of a drug sniffing dog as technology.[163]

Justice Kagan joined the majority, but in her concurrence adds that she would have found the same outcome using the *Katz* analysis and precedent in *Kyllo v. United States*,[164] which held that where the government uses technology "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…"[165] Justice Kagan says she would have found that the police used technology not in general public use (the drug sniffing dog) to explore details of the home.[166]

The dissenting Justices in *Jardines*, including the Chief Justice and Justice Kennedy, found there was no physical trespass. Notably, the dissent did not consider the dog to be technology; rather the dissenters said there was nothing that constituted trespass by bringing the dog to Jardines's front porch because "dogs have been domesticated for about 12,000 years."[167]

Jardines, like the *Jones* decision before it, provides little guidance to the electronic surveillance quagmire because it uses a property based approach, and thus, arguably does not apply to technology capable of determining information without physical intrusion upon property. Additionally, Justice Kagan's concurrence and reliance on *Kyllo*, where the Court relied upon the consideration of whether the thermal imaging technology at issue was readily available to the public, demonstrates another weakness in the Court's privacy jurisprudence: today, technology in general public use evolves so rapidly that previously expensive, highly invasive electronic surveillance technologies rapidly become cheap, readily available, and mainstream. This rule cannot form the basis of whether a form of surveillance technology is constitutionally permissible because it does not take into account the astounding pace of technological developments. It creates an unsustainable and uncertain legal rule if followed, because it would hold in one year a technology not in general public use to be constitutionally impermissible, yet advancements that made the technology readily available to the public one

---

[160] *Id*. The Court noted that "[t]he dog had been trained to detect the scent of marijuana, cocaine, heroin, and several other drugs, indicating the presence of any of these substances through particular behavioral changes recognizable by his handler." *Id*.
[161] *Id*.
[162] *Id*. at1417.
[163] *Id*. at 1417.
[164] 533 U.S. 27 (2001).
[165] *Jardines*, 133 S. Ct. at XX (Kagan, J. concurring) (quoting Kagan *Kyllo*, 533 U.S. at40).. *Kyllo* involved the warrantless use of a thermal imaging device on one's home, which the Court found to be unconstitutional.
[166] *Id*. at 1420
[167] *Id*.

year later would render that same illegal form of surveillance because the technology had become widely available to the public. UAVs are a perfect example of this. Five years ago, UAVs were not generally available for private commercial purchase on the Internet. Today, run a Google search using "drones for sale" as your search term—any 12-year old with an Internet connection and some babysitting money can find a drone readily available for inexpensive purchase on the Internet.

It is these discrepancies which demonstrate that the property based approach and other judicial precepts to determine whether use of surveillance technology is constitutional (such as the third party doctrine or the readily available to the public consideration) are not capable of creating clear precedent for courts; more importantly they fail to give clear guidance to law enforcement on appropriate uses for emerging technologies. These approaches have been acknowledged to be inadequate by the very judges struggling to address and limit the capabilities of rapidly evolving modern surveillance technologies that permit highly invasive, intrusive and surreptitious electronic surveillance.

12. <u>Maryland v. King – DNA check swab following arrest</u>

This June 2013 in a 5-4 decision, the Supreme Court ruled in *Maryland v. King* that taking and analyzing a cheek swab of an arrestee's DNA following an arrest based upon probable cause was reasonable under the Fourth Amendment.[168] The Court weighed the government interest in collecting the DNA against the privacy intrusion. Justice Kennedy, writing for the majority, found there to be a legitimate government interest in law enforcement's need "to process and identify persons and possessions taken into custody" and to be able to do so "in a safe and accurate way."[169] The majority compared the taking of DNA as a routine booking procedure, similar to fingerprinting.[170]

The majority described the collection of DNA by buccal swab as one requiring "no surgical intrusion beneath the skin" and one that poses no threat to the arrestee's health or safety.[171] Such a distinction will apply to many existing and emerging technologies, including importantly, almost all other biometric identification technology. Merely because a method of collection has improved or become less intrusive does not necessarily negate or diminish the intrusively private nature of the data collected. Fingerprinting for instance, provides a markedly sure and non-intrusive method of identifying an individual. But it does not also provide the government with intimate details about a detainees's familial blood relations, who the detainee's parents and siblings are, what a detainee's genetic makeup is, what a detainee's ancestry and country of origin is, and whether a detainee is more likely to have cancer than another individual

[168] *Maryland v. King*, 133 S. Ct. 1958, 1962 (2013).
[169] *Id*. at 1963.
[170] *Id*. at 1964.
[171] *Id*. at1963 (quoting Winston v. Lee, 470 U.S. 753, 760 (1985

UAS Legal Memoranda, continued

due to their genetic makeup. DNA collection can permit all of this to be accomplished using existing technologies.

The dissent, written by Justice Scalia, firmly and correctly condemns. He acknowledges that solving crime is a noble objective, but with this quote emphasizes the scope of search the majority has now permitted law enforcement.[172]

> Today's judgment will, to be sure, have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane (surely the Transportation Security Administration needs to know the identity of the flying public), applies for driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon[173] is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.[174]

King is yet another recent case wherein the Court struggles with rapidly involving electronic surveillance and tracking technologies and with defining protections that should be afforded individual privacy in the face of a legislative void. The Justices could not be clamoring more openly for legislative guidance.

13. *Riley v. California* (June 2014) – Search of Cellphone Incident to Arrest

In *Riley v California*,[175] the Supreme Court unanimously held that the "search incident to arrest" doctrine, which allows a police officer to search any physical object in the possession of and closely associated with the person of an arrestee, does not apply to cell phones.[176] Barring exigent circumstances, police may search an arrestee's cell phone only if they first obtain a search warrant based on probable cause.

The *Riley* Court properly based its conclusion on the nature and vast quantity of information that the typical smart phone contains – including historical cell site location information. Although neither *Jones* (discussed above) nor *Riley* squarely holds that a warrant

---

[172] *Id*. at 1989.
[173] The Panopticon was first conceived by Jeremy Bentham. The idea is a prison designed with a central guard tower that may view all inmates housed there. At the same time, the prisoners have no view of who is watching them. Eventually, the inmates modify their behavior to be in line with those who watch them. *See* Ron Collins, "*Panopticon"? –You're your eyes on the word!*, SCOTUSblog (Aug. 1, 2013, 2:02 PM), http://www.scotusblog.com/2013/06/panopticon-keep-your-eyes-on-the-word/.
[174] See *King*, 133 S. Ct. at 1989.
[175] *Riley v. California*, 573 U.S. ___ (2014).
[176] For a more thorough discussion of Riley v. California, see Chapter 28 of *Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd Ed.,* Fishman & McKenna, Thomson/West (2014 Supplement).

is needed to access either real time or historical cell phone information, those decisions point very clearly toward that conclusion.

B. U.S. Court of Appeals Decisions

1. Decisions Related to Data Collected Via Wireless

In ***Joffe v. Google***,[177] Plaintiffs filed putative class actions alleging that Google, an internet-based service provider, violated Federal Wiretap Act and state law by collecting data from unencrypted wireless local area (Wi–Fi) networks. In the course of capturing its "Street View" video for Google maps, Google's "street view" cars were equipped with sophisticated technology that not only captured video and still images, but the Google street cars also collected all unencrypted Wi-Fi data. As the Ninth Circuit described it:

> Between 2007 and 2010, Google also equipped its Street View cars with Wi–Fi antennas and software that collected data transmitted by WiFi networks in nearby homes and businesses. The equipment attached to Google's Street View cars recorded basic information about these Wi–Fi networks, including the network's name (SSID), the unique number assigned to the router transmitting the wireless signal (MAC address), the signal strength, and whether the network was encrypted. Gathering this basic data about the Wi–Fi networks used in homes and businesses enables companies such as Google to provide enhanced "location-based" services, such as those that allow mobile phone users to find nearby restaurants and attractions or receive driving directions.
>
> But the antennas and software installed in Google's Street View cars collected more than just the basic identifying information transmitted by Wi–Fi networks. They also gathered and stored "payload data" that was sent and received over unencrypted Wi–Fi connections at the moment that a Street View car was driving by. Payload data includes everything transmitted by a device connected to a Wi–Fi network, such as personal emails, usernames, passwords, videos, and documents.[178]

Google publicly apologized, but plaintiffs brought suit under federal and state law, including the Wiretap Act, 18 U.S.C. § 2511, *et seq*.. Google contended that data transmitted over a Wi–Fi network is a "radio communication" and that the Act exempts such communications by defining them as "readily accessible to the general public," 18 U.S.C. §

[177] Joffe v. Google, 729 F.3d 1262 (9th Cir. 2013), opinion amended and superseded, 2013 WL 6905957.

[178] Joffe v. Google, 729 F.3d 1262

UAS Legal Memoranda, continued

2511(2)(g)(i), so long as "such communication is not ... scrambled or encrypted," 18 U.S.C. § 2510(16)(A). Google argues that its data collection did not violate the Act because data transmitted over a Wi–Fi network is an "electronic communication" that is "readily accessible to the general public" and exempt under the Act. 18 U.S.C. § 2511(2)(g)(i).

A federal district court in California rejected Google's argument,[179] and Google appealed to the Ninth Circuit, where it argued again that the unencrypted Wi-Fi data its street view cars collected were communications that were "readily accessible to the general public." In affirming the lower court's ruling, the Ninth Circuit ruled as follows:

> We hold that the phrase "radio communication" in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi–Fi network. As a consequence, the definition of "readily accessible to the general public [ ] with respect to a radio communication" set forth in § 2510(16) does not apply to the exemption for an "electronic communication" that is "readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i).

The *Joffe* case is a civil suit, and Google is a private entity not a state actor. But the message from *Joffe* is clear: in the Ninth Circuit, police that use a UAS/UAV to intercept and collect unencrypted or encrypted Wi-Fi data without a warrant are engaging in wiretapping.

2. Decisions Related to Cellular Tracking

Since the *U.S. v Jones* GPS tracking decision, courts have grappled with cellular tracking. In *U.S. v. Skinner*, the Sixth Circuit distinguished law enforcement's cellular tracking of defendant Skinner—accomplished by continuously "pinging" Skinner's cell phone—from *Jones* because there was no physical intrusion upon Skinner's personal property. Relying on *U.S. v. Knotts*,[180] the Sixth Circuit determined that Skinner did not have a reasonable expectation of privacy in inherent location data broadcast from his cell phone.

Because Skinner was traveling on public thoroughfares and stopped at a public rest stop, the court said he had no reasonable expectation of privacy.[181] Moreover, the Sixth Circuit found no difference between trailing Skinner through physical surveillance and tracking him via cellular technology. "Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[182]

---

[179] In re Google Inc. St. View Elec. Commc'n Litig., 794 F.Supp.2d 1067, 1073–84 (N.D.Cal.2011).
[180] *U.S. v. Knotts*, 460 U.S. 276 (1983).
[181] *United States v. Skinner*, 690 F.3d 772, (6th Cir. 2012) cert. denied, 12-7971, 2013 WL 3155276 (U.S. June 24, 2013).
[182] *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012) cert. denied, 12-7971, 2013 WL 3155276 (U.S. June 24, 2013).

After the *Skinner* opinion was issued, Judge Ellen Huvelle of the United States District Court for the District of Columbia heard the *U.S. v. Jones* case on remand from the Supreme Court's remand of *U.S. v. Jones*.[183] While the case was before the Supreme Court, it ruled that the government's warrantless use of a GPS-tracking device was a physical search because of the physical intrusion/trespass involved in attaching the "slap-on" tracker to the car. But defendant Jones also argued that the government needed a warrant for his real-time, prospective cellphone data, which included location and time data, incoming and outgoing numbers dialed, but not content. The Supreme Court did not rule on this question, and Judge Huvelle considered this question on remand.

In her opinion, Judge Huvelle noted the unsettled state of the law with respect to cellphone location surveillance, and pointed out that, unlike the "slap-on" GPS tracker, cellphone location tracking does not involve physical trespass. Closely analyzing the events, Judge Huvelle noted in 2005 during the course of the Jones' investigation two federal magistrate judges in the District of Columbia had previously issued orders permitting the law enforcement to collect this data from the cellular provider without warrants. Thus Judge Huvelle ruled that the government reasonably relied upon this authority and the good faith exception applied to the warrantless. Under the good faith exception, law enforcement's warrantless collection of Jones' real-time cellphone data was permissible under the Stored Communications Act.

In *State v. Earls*,[184] however, New Jersey's Supreme Court took a decidedly different approach to cellular tracking. In *Earls*, police apprehended defendant Earls with the warrantless help of his cell phone provider, T-Mobile, which provided three sets of location data in one evening. The New Jersey Supreme Court unanimously ruled that, absent an exception, a warrant is required to obtain tracking information via cellular tracking data. The court's Judge Rabner noted that, while the text of the New Jersey Constitution is nearly identical to the Fourth Amendment, New Jersey provides greater protection against unreasonable searches and seizures than the Fourth Amendment.[185]

Characterizing cell phones as "an indispensable part of modern life"[186] and using language reminiscent of Justice Sotomayor's concurring opinion in *Jones,* Judge Rabner discussed why application of the third party doctrine[187] is inappropriate to cell phone tracking: "[c]ell phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not

[183] http://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_05-cr-00386/pdf/USCOURTS-dcd-1_05-cr-00386-9.pdf
[184] *State v. Earls*, No. A-53, (Sup. Ct. N.J. July, 18 2013).
[185] *State v. Earls*, No. A-53, slip op. at 26 (Sup. Ct. N.J. July, 18 2013).
[186] *State v. Earls*, No. A-53, slip op. at 30 (Sup. Ct. N.J. July, 18 2013).
[187] The third party doctrine articulated in *Smith v. Maryland*, 442 U.S. 735 (1979) says that one does not have a reasonable expectation of privacy in information disclosed to a third party.

UAS Legal Memoranda, continued

using a cell phone."[188] "People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with police." Even though consumers have some level of awareness that their phones can be tracked, one does not reasonably expect their precise location to be available to law enforcement without probable cause.[189]

The Tenth Circuit has addressed the constitutionality of GPS "pinging" of a suspect's cell phone to determine a suspect's location. In ***United States v. Barajas***, (10th Cir. 2013), agents prepared affidavits, which were approved to conduct wiretap surveillance on the defendant. The affidavits, however, did not include or disclose that GPS pinging would occur as to defendant's cell phone. The GPS pinging information was provided to police. The court did not decide whether pinging was a search, but pointed out that the Sixth Circuit had previously held that pinging was not a search (*Skinner)*. The court said there may not have been probable cause because the affidavit did not explain how defendant's location would reveal information about the conspiracy, but determined that the good faith exception applied. Therefore, it ruled that the GPS data was properly admitted.

One state court has taken a different approach. In ***State v. Earls***, police apprehended Earls, with the help of his cell phone provider, T-Mobile, which provided three sets of location data in one evening; a warrant was not obtained for any set of location data. The New Jersey Supreme Court held except when there is an exception, a warrant is required to obtain tracking information through the use of a cell phone. Judge Rabner wrote for a unanimous court. He first noted that while the text of the New Jersey Constitution is nearly identical to the Fourth Amendment, New Jersey provides greater protection against unreasonable searches and seizures than the Fourth Amendment.[190] The court discussed the inapplicability of the third party doctrine, reminiscent of Justice Sotomayor's concurring opinion in *Jones.*[191] "Cell phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."[192] The court also considered the nature of cell phones, which are now "an indispensable part of modern life."[193] "People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with police." Even though consumers have some level of awareness that their phones can be tracked, one does not reasonably expect their precise location to be available to law enforcement without probable cause.[194]

---

[188] *State v. Earls*, No. A-53, slip op. at 27 (Sup. Ct. N.J. July, 18 2013).
[189] *State v. Earls*, No. A-53, slip op. at 32 (Sup. Ct. N.J. July, 18 2013).
[190] *State v. Earls*, No. A-53, slip op. at 26 (Sup. Ct. N.J. July, 18 2013).
[191] The third party doctrine articulated in *Smith v. Maryland*, 442 U.S. 735 (1979) says that one does not have a reasonable expectation of privacy in information disclosed to a third party.
[192] *State v. Earls*, No. A-53, slip op. at 27 (Sup. Ct. N.J. July, 18 2013).
[193] *State v. Earls*, No. A-53, slip op. at 30 (Sup. Ct. N.J. July, 18 2013).
[194] *State v. Earls*, No. A-53, slip op. at 32 (Sup. Ct. N.J. July, 18 2013).

As the first decision of its kind, the New Jersey decision could affect state and federal court decisions when applying similar questions.

3. Decisions Related to Use of Surveillance Cameras and Videos

UAVs may easily be equipped with surveillance cameras or video recording equipment that surreptitiously capture and record still and video images that are sent back to the UAS operator. The Supreme Court aerial surveillance cases set forth above provide some framework for police in determining proper use of such electronic surveillance equipment on UAV, but lines become increasingly blurred because of the increasing sophistication of videon and audio surveillance equipment deployable via UAV. There are U.S. Court of Appeals decisions that provide some guidance in this gray area.

In ***United States v. Cuevas-Sanchez***,[195] the Fifth Circuit addressed police installation and use of a video camera installed on a utility pole (a "pole camera") overlooking a suspect's 10 foot high fenced in backyard. The officers installed the pole camera without a warrant and, using the camera, were able to observe the suspect remove drugs from the gas tanks of several cars parked in the suspect's yard. Using the evidence from the pole camera, officers obtained a warrant and arrested the defendant/suspect. At trial, the defendant moved to suppress arguing that the warrant was based on evidence obtained in violation of the Fourth Amendment, *i.e.*, the improper video search via the pole camera. The government argued that *Ciraolo* authorized this type of continuous pole camera surveillance. But the Fifth Circuit rejected this contention and found the video surveillance to be a search in violation of the Fourth Amendment. The court noted, "this was not a one-time overhead flight or a glance over the fence by a passer-by…. It does not follow that *Ciraolo* authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible."[196]

Because many UAVs, by design, can hover for extended periods of time and record video images, there is a strong analogy to the pole camera at issue in *Cuevas-Sanchez*. The prudent officer is urged to obtain a warrant when using a UAS to conduct targeted surveillance of the curtilage of a suspect's property.

In ***United States v. Wahchumwah***,[197] the Ninth Circuit considered whether an informant's use of a hidden video camera inside a home violated the Fourth Amendment. The Ninth Circuit first reviewed the core jurisprudence, stating:

---

[195] U.S. v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987).
[196] 821 F.2d at 251.
[197] U.S. v. Wahchumwah, 710 F.3d 862 (9th Cir. 2012)

UAS Legal Memoranda, continued

> "Our Fourth Amendment analysis ... ask[s] whether the individual ... has exhibited an actual expectation of privacy ... [and] whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.' " *Bond v. United States,*529 U.S. 334, 338, 120 S.Ct. 1462, 146 L.Ed.2d 365 (2000) (quoting *Smith v. Maryland,* 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)). However, that expectation of privacy does not extend to "[w]hat a person knowingly exposes to the public, even in his own home or office." *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (citations omitted).

The Ninth Circuit concluded in *Wahchumwah* that the invitee informant's use of a hidden spy cam in a suspect's home did not violate the Fourth Amendment. In so doing, the Ninth Circuit joins several other circuits that have reasoned that the one-party consent doctrine developed in audio monitoring cases also applies to secret video recording.

Advances in surveillance technology make it easy for an officer, via an UAV, to engage in audio and visual surveillance of activities and communications occurring inside a private home without an officer being anywhere near the home. Absent exigent circumstances, such use would be illegal and citizens should be assured that such use is deemed unacceptable by law enforcement.

C. Summary and Overview: How Will Courts Treat UAS/UAV Use, Searches and Data

In sum, when faced with questions about the legality of police use of UAS/UAV to monitor, to search, and to gather electronic data, a reviewing court will look closely at the facts of the situation. The reviewing court will attempt to apply the framework of existing electronic surveillance cases and the electronic surveillance statutory scheme set forth above to determine whether the use of the UAS/UAV was reasonable. Thus, police should consider beforehand the facts and circumstances that a reviewing court will review in making a determination as to the constitutionality of UAS/UAV usage, and that includes:

- the location of the search
- the specified purpose of the search or mission (routine or targeted)
- what surveillance technologies were utilized
  - were communications (verbal or electronic) intercepted
    - wiretapping statutes may apply
  - was GPS tracking or its equivalent conducted
    - *U.S. v. Jones*
  - were images taken
    - *Dow* line of cases
  - thermal imaging

- *Kyllo*
  - the sophistication of the surveillance technology used
    - what degree of imaging capabilities were employed;
    - did the UAS/UAV engage in eavesdropping of communications;
    - did the UAS/UAV mimic a cell tower and intercept electronic communications;
    - the general availability of the technology in question, etc
  - society's conception of privacy and how it would apply to the facts of the particular case.[198]

IV. CONCLUSIONS

A. Police Use of UAVs: Legally Appropriate Uses

Many of the technologies discussed above are used domestically by federal, state and local governments for a wide range of purposes and in a manner consistent with the Fourth Amendment's prohibition against unreasonable search and seizure. Federal agencies that have led the way in using such technologies include (although many scholars and attorneys hotly debate the constitutionality of certain federal agency's surveillance activities, such as the NSA): the Department of Homeland Security (DHS); the Federal Bureau of Investigation (FBI); Department of Defense (DOD); and Immigration and Customs Enforcement (ICE).

States and local police forces that routinely and appropriately employ electronic surveillance technologies include the Texas Rangers; various cities and counties in the State of Texas; various cities and counties in the State of Florida; North Dakota police; and multiple California city and county police forces. Common uses thus far—which typically do not pose constitutional and privacy concerns—include: border patrol; routine aerial patrols in rural areas (particularly effective for small offices responsible for large jurisdictions or territories); crowd surveillance; identification of vehicle via plate reader; biosurveillance; identification of individuals after criminal activities occur (Boston bomber example) and search and rescue.

Use of military UASs/UAVs by domestic law enforcement, however, raises strong constitutional concerns and arguably violates the *Posse Comitatus* Act, 18 U.S.C. § 1385, which prohibits use of military forces and equipment in domestic law enforcement.[199]

---

[198] Thompson, *CRS Drones Report* for Congress, at pg 1.
[199] Use of Army and Air Force as *posse comitatus*, 18 U.S.C. 1385, provides:
Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.

UAS Legal Memoranda, continued

B. Police Uses of UAVs that Potentially Violate the Fourth Amendment

In the absence of a warrant, use of electronic surveillance devices in a manner that would be considered to be a search under our Fourth Amendment jurisprudence is unconstitutional. There are a myriad of potential uses that would violate the Fourth Amendment. For instance, thermal imaging of buildings in public spaces may constitute a Fourth Amendment search. Listening in with acoustic enhancement to conversations that occur in public spaces but which the conversant is demonstrating a clear intent to remain private, e.g., leaning in, talking quietly or whispering, or covering mouth would likewise constitute a search.

Law enforcement employing or utilizing these devices must be familiar with and consider the Fourth Amendment principles BEFORE deploying such devices in any mission.

C. Uniform Policy and Procedure Guidelines

Advancing and emerging technologies that permit non-intrusive yet comprehensive data-gathering are here to stay. Policy, procedure and use guidelines for domestic law enforcement must consider the existing Fourth Amendment jurisprudence and provide working legal guidelines for officers when using such technologies.

By drafting uniform policy, procedure and use guidelines for domestic law enforcement in the use of such technology, domestic law enforcement can help avoid a legislative showdown, allay public fears of a "big brother" state, and help shape legislation that insures preservation of civil liberties while equipping police with Fourth Amendment compliant use of efficient, cost-effective surveillance technology.

Proactive and uniform policies with respect to: data collection, data processing, data retention, and data sharing with various federal, state and local law enforcement agencies, will reduce liability from improper data usage, improve cooperative law enforcement efforts, protect civil liberties and help shape regulation of the same. Legal Memo 3 addresses uniform data practices.

SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Legal Analysis of UAV-Collected Data: Notice, Retention, Use

TO: **The Police Foundation and the U.S. Department of Justice – COPS Office**

FROM: **Anne T. McKenna, Esquire**
Silverman|Thompson|Slutkin|White|LLC

DATE: **May 21, 2014; edited July 14, 2014**

RE: ***Community Policing and UAS Guidelines to Enhance Community Trust***
2013-CK-WX-K002
Legal Analysis of UAV-Collected Data: Notice, Retention, Use

MEMORANDUM OVERVIEW

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between The Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled "*Community Policing and UAS Guidelines to Enhance Community Trust*" (the "COPS Contract"). Pursuant to the COPS Contract Task 1 (detailed description of work appended to the COPS Contract), this memorandum ("Legal Analysis of UAV-Collected Data Practices") provides legal analysis of questions and concerns surrounding UAS/UAV-gathered electronic data, including: potentially applicable legislation; data collection; data retention; preservation of evidence; data sharing with other law enforcement; and permissible and impermissible uses of such data.

This Memo, Legal Analysis of UAV-Collected Data Practices, is structured as follows:

I. UAS-Gathered Electronic Data: Subject Introduction

UAS Legal Memoranda, continued

II. Potentially Applicable Legislation

A. The Privacy Act of 1974
B. The E-Government Act
C. Title III of the Omnibus Crime Control and Safe Streets Act (the "Wiretap Act")
D. State Legislative Example

III. Illustrative Technology-Use Guidelines: Plate Readers and Biometric ID

A. Automatic License Plate Recognition (ALPR) Technology
B. Biometric Identification Technology

IV. Data Collection Via UASs/UAVs

A. Where UAS/UAV Data Collection Takes Place
B. What Kind of Data is Collected by UAS/UAV Surveillance
C. How Much Data is Collected by UAS/UAV
D. From Whom is Data Collected by UAS/UAV

V. UAS/UAV Data Practices: Notice; Retention; and Use

A. Notice of Surveillance
B. Data Retention
i. Preservation of evidence
ii. Data Breach Laws

C. Use and Disclosure of Collected Data
i. Permissible Use and Disclosure
ii. Impermissible Use and Disclosure
iii. Interagency sharing

VI. Recommended Practices

****

I. UAS-GATHERED ELECTRONIC DATA: SUBJECT INTRODUCTION

Domestic law enforcement agencies lawfully use a myriad of electronic devices to collect electronic data about citizens. Such devices include video surveillance systems in public spaces,

GPS tracking devices,[1] and automatic license plate readers,[2] as well as devices that collect fingerprints and other biometric identifiers such as iris scans and face recognition technology.[3]

Unfortunately, little guidance exists as to how law enforcements agencies should collect, store, use and share such electronic data.[4]

The lack of legislative regulation and policy guidance is cause for concern for law enforcement agencies and for privacy advocates, but this concern is heightened and compounded when such surveillance technologies are harnessed aboard UAVs. Setting the question of UASs/UAVs aside, concerns over indiscriminate and unlimited surveillance by law enforcement and the increasingly vast amount of electronic data that result from such surveillance have been voiced in a variety of contexts. Justice Sonia Sotomayor recently shared these concerns in her concurrence to *US v. Jones*, the Supreme Court's 2012 decision on GPS monitoring:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'[5]

Because UAS/UAV can be equipped with GPS tracking technology, as well as video-recording and facial-recognition technology, the monitoring capacities of UAS/UAV thus are equally susceptible, if not more, to facilitating the limitless data collection Justice Sotomayor apprehends.

In this Memo, we analyze these legal issues and provide an overview of laws and policies that may apply to law enforcement use of UASs/UAVs. Specifically, we focus upon recommendations for data gathered by Automatic License-Plate Recognition (ALPR) technology and biometric identification technology, because these recommendations for data gathered by use of these technologies provide useful analogy to potential UAS/UAV data collection. We use the term "recommendations" because the federal government, as well as most states and localities,

---

[1] *See, e.g., United States v. Jones*, 132 S. Ct. 945 (2012)
[2] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 286-87
[3] Sabrina A. Lochner, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 Ariz. L. Rev. 201, 202 (Spring 2013).
[4] *Id.* at 202-203.
[5] *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

UAS Legal Memoranda, continued

have done little or nothing to regulate the rapidly expanding use of such technologies when deployed via UASs.[6]

II. POTENTIALLY APPLICABLE LEGISLATION

At present, no federal legislation *explicitly* regulates UAS/UAV-gathered electronic data, and little regulation exists under state law.[7] However, depending on (1) how surveillance is conducted via UAS, (2) what type of surveillance technology is utilized, and (3) what data is collected, there are potentially applicable laws as well as promulgated guidelines. We have set these federals laws forth in this section and then discuss these laws in more detail throughout Data Collected via UAVs Memo where context appropriate. Subpart D of this section discusses an example of legislation emerging at the state level to regulate UAS/UAV data collection.

A. The Privacy Act of 1974

The Privacy Act of 1974, P.L. 93-579, § 2, 88 Stat. 1896, is 40-year-old Watergate reform legislation critically in need of an overhaul. The Privacy Act seeks to ensure that individual records are disclosed and used only for a "necessary and lawful purpose."[8] Section 552a(b) of the Privacy Act enumerates a series of specific conditions under which disclosure is permissible.[9] In the absence of consent by the individual, federal agencies cannot disclose an individual's records protected by the Privacy Act to any person or any agency unless one of these specific conditions are met.[10]

B. The E-Government Act

The E-Government Act of 2002, Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803, requires federal agencies to conduct "Privacy Impact Assessments" (PIAs) prior to "developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public."[11] A PIA must analyze what information is collected; when, how, and why this information is collected; disclosure and security of collected information; and "should address the impact the system will have on an

[6] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 286-87 (noting that legislative regulation of indiscriminate data collection by ALPR does exist in New Hampshire and Maine, but remains generally unregulated nationwide).
[7] See Sect. III.D. for an example of state legislation.
[8] Privacy Act of 1974, Congressional Findings and Statement of Purpose, Act of Dec. 31, 1974, P.L. 93-579, § 2, 88 Stat. 1896.
[9] 5 U.S.C. § 552(a)(b).
[10] 5 U.S.C. § 552(a)(b).
[11] Memorandum from Joshua B. Bolten, Director, Office of Mgmt. and Budget to Heads of Executive Departments and Agencies, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), available at http://www.whitehouse.gov/omb/memoranda/m03-22.html; Jeremy Brown, Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places, 23 Berkeley Tech. L.J. 755, 781 (2008).

individual's privacy."[12] However, this provides little in the way of substantive regulation or guidance on issues related to the actual implementation of such technology.

Section 208 of the E-Government Act requires careful consideration: Section 208 establishes Government-wide requirements for conducting, reviewing, and publishing PIAs. The Department of Defense (DOD) provides some helpful guidance in the use of new Information Technology (IT) systems, although DOD's guidance is directed to DOD-affiliated agencies or "components." As summarized by the Defense Logistics Agency (DLA), Section 208 of the E-Government Act requires DOD components:

> [T]o conduct reviews of how privacy issues are considered when purchasing or creating new Information Technology (IT) systems or when initiating new electronic collections of information in personally identifiable form. A PIA addresses privacy factors for all new or significantly altered Information Technology (IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public - excluding information on DoD personnel). The OMB government-wide guidance directs all federal agencies, including the Department of Defense, to conduct PIAs on a slightly broader category of individuals, i.e., including contractors. Therefore, the DLA guidance mirrors the OMB government-wide guidance and adheres to this standard.[13]

Given that UASs/UAVs are "IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public," the E-Government Act provides useful guidance for non-federal domestic law enforcement in terms of conducting PIAs before implementing a UAS program, and it also provides useful guidance in terms of data collection and interagency data sharing.

C. Title III of the Omnibus Crime Control and Safe Streets Act (the "Wiretap Act")

Title III of the Omnibus Crime Control and Safe Streets Act (the "Wiretap Act")[14] is instructive with regards to UAV/UAS surveillance that utilizes audio- or video-recording devices. The ABA Standards on Technologically-Assisted Physical Surveillance, while not legally binding, also provide useful guidance on this topic.[15] The following sections will review the applicability of existing federal legislation and legal principles to UAS/UAV-gathered

[12] Id.
[13] Def. Logistics Agency, *E-Government Act of 2002 (Privacy Impact Assessments)*, http://www.dla.mil/foia-privacy/Pages/eGovernment.aspx (last visited May 20, 2014).
[14] 18 U.S.C. §§ 2510-2522.
[15] American Bar Association, *Standards for Criminal Justice-Electronic Surveillance* (3d ed.), Section B: Technologically-Assisted Physical Surveillance (hereafter ABA Standards).

UAS Legal Memoranda, continued

electronic data in terms of issues related to data collection, data retention, and data use and disclosure.

D. State Legislative Example

Some examples of regulation of UAS/UAV-gathered electronic data have emerged at the state level in recent years.[16] The most specific example of state legislation targeting UAS/UAV surveillance by law enforcement is Illinois's "Freedom from Drone Surveillance Act."[17] The Act explicitly addresses police surveillance and data collection via UAS/UAV, stating that "a law enforcement agency may not use a drone to gather information."[18] Information is defined by the Act as "any evidence, images, sounds, data, or other information gathered by a drone."

The Act's general ban on law enforcement agencies' use of UAS/UAV to gather information is subject to five specific exceptions. Agencies may use UAS/UAV:

(1) In response to terrorist threats;

(2) After first obtaining a search warrant;

(3) For a period of 48 hours during emergency situations;

(4) To locate a missing person, if such activity is separate from a criminal investigation; and

(5) To photograph crime scenes and traffic crashes, provided that the scope of such photography is sufficiently limited.[19]

Retention and disclosure of UAS/UAV-gathered information is explicitly limited under the Act. Where a law enforcement agency deploys UAS/UAV pursuant to one of these authorized uses, "the agency within 30 days shall destroy all information gathered by the drone."[20] Agency supervisors are granted limited authority to retain information beyond 30 days "if (1) there is reasonable suspicion that the information contains evidence of criminal activity, or (2) the information is relevant to an ongoing investigation or pending criminal trial."[21] The authority to disclose this information is also granted solely to agency supervisors, who can share information

[16] For a more comprehensive overview of current state regulation of UAS/UAV use, see the Police Foundation's State Legislation Memorandum and this Firm's State Legislation Chart summarizing and depicting state laws and municipal ordinances pertaining to or proscribing UAS use in general and with respect to law enforcement use.
[17] S.B. 1587, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), *available at* http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=85&GA=98&DocTypeId=SB&DocNum=1587&GAID=12&LegID=72407&SpecSess=&Session=.
[18] S.B. 1587.
[19] Id.
[20] Id.
[21] Id.

with another government agency only when the information contains evidence of criminal activity or is relevant to an ongoing investigation or criminal trial.[22]

Information obtained by law enforcement use of UAS/UAV in violation of the Act is inadmissible in judicial and administrative proceeding.[23]

III. ILLUSTRATIVE TECHNOLOGY-USE GUIDELINES: PLATE READERS AND BIOMETRIC ID

A. Automatic License Plate Recognition (ALPR) Technology

The privacy and data retention concerns raised by ALPR technology are similar to those raised by UAS/UAV surveillance, particularly with respect to the specter of indiscriminate collection and limitless retention of data pose by both technologies. Law enforcement agencies are increasingly utilizing ALPR systems to track vehicle movements. ALPRs can be mounted on patrol cars, toll booths, and along access roads, and the systems are capable of rapidly recording vast amounts of data about the movements of both criminal and innocent citizens.[24] Despite the apparently widespread use of ALPRs and the potential for limitless data retention and aggregation, this technology is largely unregulated. Self-imposed data retention policies vary widely. For example, the Drug Enforcement Agency (DEA) retains ALPR-collected data for up to two years and shares this information with other federal agencies and local police.[25] The New York State Police retains ALPR-collected data indefinitely.[26]

In 2009, the International Association of Chiefs of Police (IACP) published its Privacy Impact Assessment Report for the Utilization of License Plate Readers.[27] The report recognized the lack of uniform rules or guidelines governing the appropriate use and sharing of ALPR data and noted that "potential misuse of LPR data may expose agencies operating such systems to civil liability and negative public perceptions."[28] In light of these concerns, IACP's goal for the report was to identify "the impact LPR systems can have on the public's privacy interests and to make recommendations for the development of information management policies intended to

---

[22] Id.
[23] Id.
[24] Hilary Hylton, License-Plate Scanners: Fighting Crime or Invading Privacy?, TIME (July 30, 2009), available at http://content.time.com/time/nation/article/0,8599,1913258,00.html.
[25] G. W. Schulz, "DEA Installs License-plate Recognition Devices Near Southwest Border," Ars Technica, July 11, 2012, available at http://arstechnica.com/tech-policy/2012/07/dea-installs-license-plate-recognition-devices-near-southwest-border/.
[26] Cyrus Farivar, "Your Car, Tracked: The Rapid Rise of License Plate Readers," Ars Technica, September 27, 2012, available at http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/.
[27] International Association of Chiefs of Police, Privacy impact assessment report for the utilization of license plate readers (2009), available at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf (hereafter IACP Report).
[28] IACP Report at 1.

UAS Legal Memoranda, continued

govern an agency's operation of a LPR system."[29] The report suggested that LPR data can be appropriately accessed to conduct crime analysis, to alert officers of the location of a license plate that has been included on a "hot list," and to detect criminal conduct.[30] Sharing of LPR data may be appropriate among law enforcement agencies; other, non-law enforcement government entities; and with the public in specific, limited circumstances.[31] IACP recommends that data retention policies should consider issues including:

- Statutes of limitation
- Potential future usefulness of the data
- Sensitivity of the data
- The system's technologically implemented policy controls.[32]

The IACP report emphasizes that, while there is no standard formula for determining retention policies, it is critical that a standard policy is established and followed.[33]

Undersigned counsel recommends that data retention policies also specify:

- Retention period: Length of data retention
- Data storage: how data is stored, secured and protected
- Access: who may access the retained data and under what circumstances
- Use: for what purposes may the data lawfully be used
- Disclosure: to what other persons or agencies may the data be disclosed

B. Biometric Identification Technology

Recommendations for police use of biometric identification technology are instructive for UAS/UAV use, particularly because UAS/UAV can be equipped with biometric identification technology, including facial recognition technology. A prominent example of this technology is the Mobile Offender Recognition and Information System ("MORIS"). MORIS is a smartphone-based mobile device capable of identifying individuals via facial recognition technology, iris scans, and fingerprints.[34] When used with an iPhone, the device can photograph an individual's face and check the image against a criminal records database maintained by the device's manufacturer.[35] MORIS does not presently store these images, but there is nothing preventing

[29] IACP Report at 1.
[30] Id at 3.
[31] Id.
[32] Id at 4.
[33] Id.
[34] See Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 202 (2013).
[35] Zach Howard, Police to Begin iPhone Iris Scans Amid Privacy Concerns, Reuters (July 20, 2011, 2:59 PM).

this in the future.[36] MORIS is reportedly employed by more than 50 law enforcement agencies nationwide, but there is a concerning lack of regulation regarding how officers should collect, retain, use and disclose data with this device.[37]

One law review article identifies a troubling distinction between stationary surveillance devices, such as ALPR and video cameras attached to fixed locations, and mobile surveillance devices, such as MORIS or UAVs. The mobility of a surveillance device permits police discretion in whom to scan or record, which can produce discriminatory surveillance results.[38]

IV. DATA COLLECTION VIA UAS/UAV

Law enforcement collection[39] of electronic data via surveillance devices deployed on UAS/UAV must address four principal concerns:

(1) where the data collection takes place;

(2) what kind of data is being collected;

(3) how much data is collected; and

(4) from whom is the data being collected.

The following subsections address each of these concerns.

A. Where UAS/UAV Data Collection Takes Place

As discussed in Legal Memo #1, the Fourth Amendment does not require law enforcement to obtain a search warrant before installing and utilizing video equipment and cameras to record activities exposed to the public and visible to the naked eye.[40] The area under

[36] Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 225 (2013).
[37] Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 202 (2013)
[38] Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 218-19 (2013).
[39] This section addresses only *data collection* issues. Data retention is addressed in Section III and Section V. Data use is addressed in Section V as well.
[40] *See, Dow Chem. Co. v. United States*, 476 U.S. 227, 239, 106 S. Ct. 1819, 1827, 90 L. Ed. 2d 226 (1986) (holding that aerial surveillance from navigable airspace does not violate the Fourth Amendment); *California v. Ciraolo*, 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) ("The Fourth Amendment protection of the home has never extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.").

UAS Legal Memoranda, continued

surveillance must be visible from a lawful vantage point,[41] and the surveillance must record only what passersby could otherwise observe.[42]

B. What Kind of Data is Collected by UAS/UAV Surveillance

Law enforcement surveillance operations that employ UAS/UAV equipped with audio- or video-recording capabilities may be subjected to regulation by Title III of the Wiretap Act if the data collected includes wire or oral communications protected by that Act. Determining whether UAS/UAV surveillance falls within the scope of Title III requires a two-step inquiry. First, the agency must determine whether the surveillance technology is capable of intercepting wire, oral or electronic communications. Section 2510 defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[43] Second, the agency must determine whether the surveillance technology may intercept communications protected by Title III. An "oral communication" within the scope of Title III is defined as a communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectations."[44] In other words, the speaker must have a "reasonable expectation of privacy" in the conversation in order to constitute an "oral communication" protected by Title III.[45] Thus, UAS/UAV surveillance equipped with technology capable of audio-recording private conversations is subject to Title III.

Where UAS/UAV surveillance intercepts and records protected wire or oral communications, officers must obtain surveillance authorization pursuant to Title III. Unauthorized collection of such protected data is a violation of Title III, for which exclusionary sanctions and other penalties may result.[46]

It is important to note that law enforcement use of video surveillance is not, to date, explicitly regulated by federal statute. Courts have suggested that Title III of the Wiretap Act may nevertheless be implicated in such activity, specifically due to audio-recording capabilities of video surveillance and generally in light of underlying public policy of the Act.[47] Title III

[41] *California v. Ciraolo*, 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986).
[42] *United States v. Jackson*, 213 F.3d 1269, 1281 (10th Cir. 2000) cert. granted, judgment vacated on other grounds, 531 U.S. 1033, 121 S. Ct. 621, 148 L. Ed. 2d 531 (2000) (noting that video cameras installed on public telephone poles "were incapable of viewing inside the houses, and were capable of observing only what any passerby would easily have been able to observe.").
[43] 18 U.S.C. § 2510(4).
[44] 18 U.S.C. § 2510(2).
[45] *United States v. Harrelson*, 754 F.2d 1153, 1170 (5th Cir. 1985)
[46] 18 U.S.C. § 2511
[47] *See United States v. Nerber*, 222 F.3d 597, 604-05 (9th Cir. 2000) ("Although no federal statute regulates the government's use of video surveillance, the existence of a law which prohibits the warrantless use of audio surveillance on a citizen alone in another person's hotel room is strong evidence that society is not prepared to accept the warrantless use of an even more intrusive investigative tool in the same situation.").

likely does not govern silent video camera surveillance.[48] However, where video camera surveillance collects both visual and audio data, the audio portion of the surveillance may constitute interception of wire and oral communications under Title III.[49] Courts have suggested that, as long as officers conduct video surveillance in conformity with Title III requirements, they have complied with the Fourth Amendment warrant clause as well.[50]

C. How Much Data is Collected by UAS/UAV

Law enforcement should ensure that UAS/UAV data collection is sufficiently limited in scope. The Supreme Court has suggested that the Fourth Amendment universally requires a reasonably limited scope for surveillance activity.[51] Pervasive and limitless UAV/UAS surveillance and data collection thus may violate the Fourth Amendment due to its unreasonably broad scope.

Title III of the Wiretap Act explicitly requires surveillance to be limited in scope. Where Title III regulates UAS/UAV surveillance, law enforcement must "minimize the interception of communications not otherwise subject to interception" or otherwise outside of the scope of authorization.[52] The American Bar Association's Standards on Technologically-Assisted Physical Surveillance also indicates that the "scope of the surveillance should be limited to its authorized objectives and be terminated when those objectives are achieved."[53]

D. From Whom is Data Collected by UAS/UAV

Law enforcement must avoid discriminatory collection of data by UAS/UAV. Searches and seizures based on racial discrimination may violate the Equal Protection Clause of the Fourteenth Amendment.[54] The ABA Standards also indicates that "subjects of the surveillance should not be selected in an arbitrary or discriminatory manner."[55] Research on the United Kingdom's video surveillance system revealed bias against minorities and "massively disproportionate targeting of young males, particularly if they are black or visibly identifiable as having subcultural

---

[48] *U.S. v. Larios*, 593 F.3d 82, 90 (1st Cir. 2010); *U.S. v. Jackson*, 213 F.3d 1269, 1280 (10th Cir. 2000), cert. granted, judgment vacated on other grounds, 531 U.S. 1033, 121 S. Ct. 621, 148 L. Ed. 2d 531 (2000); *U.S. v. Taketa*, 923 F.2d 665, 675 (9th Cir. 1991)
[49] *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984).
[50] *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984) ("If the government conducts television surveillance in conformity with the requirements of particularity that Title III imposes on electronic eavesdropping (not literal conformity, of course, since words such as "communications" and "intercept" in Title III do not fit television surveillance), the government has also conformed to the requirement of particularity in the Fourth Amendment's warrant clause.").
[51] *Terry v. Ohio*, 392 U.S. 1, 17-19, 88 S. Ct. 1868, 1878, 20 L. Ed. 2d 889 (1968) ("This Court has held in the past that a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope.").
[52] 18 U.S.C. § 2518(5)
[53] ABA Standards, supra note 5.
[54] *Whren v. United States*, 517 U.S. 806, 813, 116 S. Ct. 1769, 1774, 135 L. Ed. 2d 89 (1996)
[55] ABA Standards, supra note 5.

UAS Legal Memoranda, continued

affiliations."[56] The potential for discriminatory targeting may be inherent to such large-scale public surveillance operations, and law enforcement must take proper steps to prevent such unlawful conduct.

V. UAS/UAV DATA PRACTICES: NOTICE; RETENTION; AND USE

A. Notice of Surveillance

Law enforcement conducting surveillance via UAS/UAV may also be required to provide notice of the surveillance. Where surveillance is conducted pursuant to judicial authorization, both Title III of the Wiretap Act and the ABA Standards indicate that post-surveillance notification must be given to all individuals listed on the warrant application for communication surveillance.[57] Where crime deterrence is the primary goal, pre-surveillance notification will not only help further that goal but also minimize potential unexpected intrusions on privacy.[58] The ABA Standards also recommend giving such pre-surveillance notice.[59]

B. Data Retention

In light of technological advances that have facilitated low-cost, high-volume storage data, both courts and legal commentators have expressed concern over the lack of regulations on surveillance data retention.[60] A federal judge for the Ninth Circuit Court warned of GPS tracking capability to "create a permanent electronic record that can be compared, contrasted and coordinated to deduce all manner of private information about individuals. By holding that this kind of surveillance doesn't impair an individual's reasonable expectation of privacy, the panel hands the government the power to track the movements of every one of us, every day of our lives."[61]

As one commentator has noted, in the absence of meaningful regulation "law enforcement is arguably incentivized to take advantage of the declining costs of storage by creating 'digital dossiers' to aid in future investigations."[62] The D.C. Circuit Court recognized that "[a] reasonable person does not expect anyone to monitor and retain a record of every time he drives

---

[56] Clive Norris & Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* 212-14 (1999), at 50; Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 298-99 (2002).
[57] 18 U.S.C. § 2518(8)(d); ABA Standards, supra note 18.
[58] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 297-98 (2002).
[59] ABA Standards, supra note 5.
[60] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 291.
[61] *United States v. Pineda–Moreno*, 617 F.3d 1120, 1125 (C.A.9 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).
[62] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 291.

his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'"[63]

Notably, one manufacturer of facial recognition technology recommended "reasonable uses principles" for its systems, which included a "No Match-No Memory" practice "to ensure that no audit trail is kept of faces that do not match a known criminal or a person under active police investigation." The manufacturer further advised that "[n]on-matches should be purged instantly."[64]

The Freedom from Drone Surveillance Act, passed by the Illinois state legislature in 2013, provides an example of recommended data retention and data use practices.[65] As discussed in Section II of this memo, the Act prohibits retention of information gathered by law enforcement via UAS/UAV beyond 30 days, unless the information contains evidence of criminal activity or is relevant to an ongoing criminal investigation or trial.[66] Information gathered by UAS/UAV may not be disclosed under the Act unless it meets the same criteria for retention beyond 30 days.[67]

i. Preservation of evidence

Given the absence of meaningful regulation on the retention of electronic data collected by electronic surveillance, the primary concern for law enforcement in this context is data security and preservation of evidence.

Title III of the Wiretap Act requires that authorized recordings of intercepted communications must be protected from editing or alterations and sealed under judicial order.[68] Custody of the recordings is directed by judicial order and the records must be kept for ten years, unless court order directs otherwise.[69]

ii. Data Breach Laws

---

[63] *United States v. Maynard*, 615 F.3d 544, 563 (D.C. Cir. 2010) (quoting *Nader v. Gen. Motors Corp*., 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring))), cert. granted sub nom. *United States v. Jones*, 131 S. Ct. 3064 (2011) (No. 10-1259).
[64] Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to A World That Tracks Image and Identity*, 82 Tex. L. Rev. 1349, 1473 (2004) (citing recommended "reasonable use principles" issued by Visionic, a manufacturer of facial recognition technology).
[65] S.B. 1587 (Ill. 2013). For a more detailed discussion of The Freedom from Drone Surveillance Act, see Section II of this memo.
[66] S.B. 1587.
[67] S.B. 1587 ("[T]he agency shall not disclose any information gathered by the drone, except that a supervisor of that agency may disclose particular information to another government agency, if (1) there is reasonable suspicion that the information contains evidence of criminal activity, or (2) the information is relevant to an ongoing investigation or pending criminal trial.").
[68] 18 U.S.C. § 2518(8)(a).
[69] 18 U.S.C. § 2518(8)(a).

UAS Legal Memoranda, continued

At present, no universally applicable federal law regulates data breach notification. State-level regulation, however, is widespread. Currently, forty-six states and the District of Columbia impose notification requirements for breaches of personal information data.[70] Several of these state laws exempt government agencies from complying with notification requirements, directing application to "businesses" or "persons."[71] Other state laws, importantly California's Security Breach Information Act,[72] *do* apply to "agencies." However, several states that require government agencies to notify individuals of data breaches also specifically exempt these agencies from being punished for non-compliance.[73]

In the absence of a state data breach law that applies to and is enforceable against government agencies, constitutional privacy rights may provide grounds for recovery of damages due to government data breach. The Supreme Court has suggested the possibility of "a threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[74] One legal commentator has suggested that a government data breach which violates the right to informational privacy could give rise to a section 1983 claim against the state or a *Bivens* action against the officer.[75] The likelihood of success with either approach is low, however, as the Supreme Court has established several doctrines regarding these claims that create significant obstacles to recovery.[76]

In addition to applicable state law on data breach, three federal statues provide useful guidelines for law enforcement agencies in developing data security and breach notification policies. The Privacy Act of 1974 and the E-Government Act of 2002 require federal agencies to protect and ensure the security of personal information.[77] The Federal Information Security

---

[70] See Reid J. Schar and Kathleen W. Gibbons, Complicated Compliance: State Data Breach Notification Laws, BLOOMBERG (Aug. 9, 2013), available at http://www.bna.com/complicated-compliance-state-data-breach-notification-laws/.

[71] For example, Connecticut, Georgia, Maryland, Montana, North Dakota, Texas, and Utah's statutes define breach with this language. Conn. Gen. Stat. Ann. §36a-701b(b) (West Supp. 2009); Ga. Code Ann. §10-1-911(2) (2009); Md. Code Ann., Com. Law § 14-3501 (2008); Mont. Code. Ann. §30-14-1704(1) (2009); N.D. Cent. Code. §51-30-02 (2007); Tex. Bus. & Com. Code Ann. §521.053(a) (Vernon Supp. 2009); Utah Code Ann. §13-33-202 (2005). See Jill Joerling, Data Breach Notification Laws: An Argument for A Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J.L. & Pol'y 467, 476 (2010).

[72] California Security Breach Information Act §1798.29.

[73] See Jill Joerling, Data Breach Notification Laws: An Argument for A Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J.L. & Pol'y 467, 476 (2010) (identifying Florida, Hawaii, Maine, and Tennessee as specifically excluding government agencies from enforcement proceedings).

[74] Whalen v. Roe, 429 U.S. 589, 605, 97 S. Ct. 869, 879, 51 L. Ed. 2d 64 (1977)

[75] A. Michael Froomkin, Government Data Breaches, 24 Berkeley Tech. L.J. 1019, 1054-55 (2009). See Legal Memo #2 for a detailed explanation of section 1983 claims and *Bivens* actions.

[76] A. Michael Froomkin, Government Data Breaches, 24 Berkeley Tech. L.J. 1019, 1052 (2009).

[77] See U.S. Gov't Accountability Office, Information Security: Protecting Personally Identifiable Information, GAO 08-343, at 13 (Jan. 2008), available at http://www.gao.gov/new.items/d08343.pdf.

Management Act of 2002 (FISMA) also requires federal agencies to "develop, document, and implement an agencywide information security program."[78]

The Privacy Act, which applies only to federal government agencies, limits agencies' collection, disclosure, and use of personally identifiable information maintained in a record system.[79] Notably, the Privacy Act regulates only intentional disclosure of personal information.

The E-Government Act requires agencies to conduct privacy impact assessments (PIA) to analyze how information technology systems manage and protect personal information.[80]

FISMA directs agencies to conduct a risk-based assessment of information security management and to "cost-effectively reduce information security risks to an acceptable level."[81] Federal agencies are also required to provide security awareness training to personnel, conduct periodic testing of the security measures, and implement "procedures for detecting, reporting, and responding to security incidents."[82] In responding to security incidents, agencies may notify the Federal information security center, law enforcement agencies, national security agencies, or any other designated agency or office.[83] FISMA authorizes the central Federal information center to provide information and technical assistance to operators of agency information systems and to consult with other federal agencies as appropriate.[84]

FISMA does not specifically address notification to members of the public, but the U.S. Office of Management and Budget (OMB) has included this requirement in its directive on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[85] As of 2007, federal agencies are required to implement a "breach notification policy" that includes external breach notification. Specifically, OMB requires that "Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification."[86]

C. Use and Disclosure of Collected Data

[78] 44 USC § 3544(b).
[79] See U.S. Gov't Accountability Office, Information Security: Protecting Personally Identifiable Information, GAO 08-343, at 13 (Jan. 2008), available at http://www.gao.gov/new.items/d08343.pdf.
[80] See U.S. Gov't Accountability Office, Information Security: Protecting Personally Identifiable Information, GAO 08-343, at 13 (Jan. 2008), available at http://www.gao.gov/new.items/d08343.pdf.
[81] 44 USC § 3544(b).
[82] 44 USC § 3544(b).
[83] 44 USC § 3544(b)(7).
[84] 44 USC § 3546.
[85] Memorandum from Clay Johnson III, Deputy Dir. For Mgmt., Office of Mgmt. & Budget, on Safeguarding Against and Responding to the **Breach** of Personally Identifiable Information, M-07-16 (May 22, 2007), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.
[86] Memorandum from Clay Johnson III, Deputy Dir. For Mgmt., Office of Mgmt. & Budget, on Safeguarding Against and Responding to the **Breach** of Personally Identifiable Information, M-07-16, at 19 (May 22, 2007), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

UAS Legal Memoranda, continued

Disclosure of information can, in itself, constitute an invasion of privacy.[87] The Supreme Court has further noted "the fact that an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[88] In addition to addressing Constitutional concerns, law enforcement's use and disclosure of data gathered by UAS/UAV must also consider Title III of the Wiretap Act, the Privacy Act of 1974, and the Freedom of Information Act exemption 7(c). The following section will first address permissible use and disclosure of UAS/UAV-gathered data in light of existing legal regulations, followed by a discussion of impermissible use and disclosure.

i. Permissible Use and Disclosure

Title III of the Wiretap Act and the ABA Standards suggest general consensus that surveillance data may be used and disclosed exclusively for law enforcement purposes, unless exigent circumstances warrant otherwise.

Where law enforcement officers have intercepted wire, oral, or electronic communications by means authorized by Title III, § 2517(1) of that statute authorizes law enforcement officers to disclose the contents of these communications to other officers to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.[89] This provision permits the exchange of information obtained from lawfully intercepted communications among law enforcement officers and between state and federal law enforcement agencies.[90] Such an exchange is permissible only to the extent that it is appropriate to the proper performance of the official duties of both the officer making and the officer receiving the disclosure.[91]

Section 2517(2) of Title III permits law enforcement who have learned of the contents of lawfully intercepted communications to "use such contents to the extent such use is appropriate to the proper performance of his official duties."[92] Appropriate use of intercepted communications may include establishing probable cause for arrest or search warrants and developing additional investigative leads.[93]

Law enforcement conducting surveillance in compliance with Title III may inevitable intercept communications related to offenses outside the scope of the Title III authorization

[87] Martin Marcus, Christopher Slobogin, *ABA Sets Standards for Electronic and Physical Surveillance*, Crim. Just., Fall 2003, at 5, 17
[88] *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 770, 109 S. Ct. 1468, 1480, 103 L. Ed. 2d 774 (1989)
[89] 18 USC § 2517(1)
[90] S. Rep. 90-1097, at 2188. See also, *2 Law of Electronic Surveillance* § 7:34
[91] 18 USC § 2517(1)
[92] 18 USC § 2517(2).
[93] S. Rep. 90-1097, at 2188. See also, *2 Law of Electronic Surveillance* § 7:36

order. Section 2517(5) makes clear that the contents of those communications can also be disclosed and used as provided in § 2517(1) and (2).[94]

Section 2517(3) of Title III permits admission of lawfully intercepted wire, oral, or electronic communications in court proceedings.[95] Privileged communications that are otherwise lawfully intercepted retain their privileged character.[96] Communications intercepted in violation of Title III and any evidence derived therefrom cannot be admitted into evidence at any court proceeding or before any legislative committee or Federal or State government authority.[97] While the language of § 2515 indicates a complete prohibition on any use of unlawfully intercepted communications as evidence, the legislative history of Title III suggests possible Congressional intent that such communications could be used for impeachment purposes.[98]

Law enforcement officers can disclose communications to certain federal government officials "to the extent that such contents include foreign intelligence or counterintelligence" where this information will assist the official in performing official duties.[99] Disclosure can also be made to foreign law enforcement as it relates to the recipient's official duties.[100] Finally, law enforcement may disclose to any appropriate federal, State, local or foreign official communications related to threats of terrorism or hostile acts by a foreign power.[101]

The Privacy Act of 1974 seeks to ensure that individual records are disclosed and used only for a "necessary and lawful purpose."[102] Section 552a(b) of the Privacy Act enumerates a series of specific conditions under which disclosure is permissible.[103] In the absence of consent by the individual, federal agencies cannot disclose an individual's records protected by the Privacy Act to any person or any agency unless one of these specific conditions are met.[104]

ii. Impermissible Use and Disclosure

Both Title III of the Wiretap Act and the ABA Standards indicate that use and disclosure of UAS/UAV-gathered electronic data should be prohibited for any purpose not related to

[94] 18 USC § 2517(5)
[95] 18 USC § 2517(3)
[96] 18 USC § 2517(4)
[97] 18 USC § 2515
[98] S. Rep. 90-1097. See also *2 Law of Electronic Surveillance* § 7:81 (The formal legislative history of Title III, Senate Report 1097, indicates that illegally obtained recordings may be available for impeachment purposes, by stating that the exclusionary provision of § 2515 is not intended "to press the scope of the suppression role beyond present search and seizure law.")
[99] 18 USC § 2517(6).
[100] 18 USC § 2517(7)
[101] 18 USC § 2517(8)
[102] Privacy Act of 1974, Congressional Findings and Statement of Purpose, Act of Dec. 31, 1974, P.L. 93-579, § 2, 88 Stat. 1896.
[103] 5 U.S.C. § 552(a)(b).
[104] 5 U.S.C. § 552(a)(b).

UAS Legal Memoranda, continued

official law enforcement duties.[105] In addition, the Freedom of Information Act (FOIA) exemption 7(c) prohibits federal disclosure of "investigatory records compiled for law enforcement purposes" when such disclosure would "constitute an unwarranted invasion of personal privacy."[106] The Supreme Court has recognized that protecting privacy interests includes "the individual interest in avoiding disclosure of personal matters."[107] The Court determined that this interest was implicated by a FOIA request for a citizen's FBI rap sheet, concluding that disclosure of the rap sheet was protected by FOIA Exemption 7(c). The Court rejected the requesting party's argument that the citizen held no privacy interest in the rap sheet because the events summarized therein had previously been disclosed to the public.[108] Notably, the Court characterized this argument as a "cramped notion of personal privacy."[109]

Unfortunately, abuse of surveillance data captured by UAV is a credible concern. For example,[110] in 2004 a New York City police surveillance video captured the suicide of a twenty-two year old man in the lobby of a public housing unit.[111] After a New York City police officer shared the recording with a friend, the video appeared on an offensive online forum.[112] The tort of public disclosure of private facts is increasingly recognized by state courts and may create liability for officers engaging in such offensive conduct.[113]

iii. Interagency sharing

Officers may be able to share UAS/UAV-gathered data with other federal, state, and local governmental agencies where such data contains foreign intelligence or law enforcement information that is relevant to the receiving agency's official duties. The USA PATRIOT Act includes several provisions to facilitate increased sharing of foreign intelligence and law enforcement information.[114] Section 203 of the PATRIOT Act grants broad authority to share foreign intelligence information gathered during criminal investigations with certain federal

---

[105] 18 U.S.C. § 2517; ABA Standards, supra note 5.
[106] 5 USC § 552(b)(7)(c)
[107] *Whalen v. Roe*, 429 U.S. 589, 598-600, 97 S.Ct. 869, 875-877, 51 L.Ed.2d 64 (1977) (footnotes omitted).
[108] *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 762-63, 109 S. Ct. 1468, 1476, 103 L. Ed. 2d 774 (1989).
[109] *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 762-63, 109 S. Ct. 1468, 1476, 103 L. Ed. 2d 774 (1989).
[110] Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 Berkeley Tech. L.J. 755, 763-64 (2008) (discussing the 2004 story of Paris Lane's suicide and police abuse of surveillance recording of that event).
[111] Shaila K. Dewan, *Video of Suicide in Bronx Appears on Shock Web Site*, N.Y. Times, Apr. 1, 2004, at B3.
[112] Murray Weiss, Bx. *Cop Caught in 'Net--Suicide-Video Scandal*, N.Y. Post, June 22, 2004, at 25.
[113] See Restatement (Second) of Torts § 652D (1977).
[114] See Richard A. Best Jr., Sharing Law Enforcement and Intelligence Information: The Congressional Role Summary, Congressional Research Service (Feb. 13, 2007), available at http://www.fas.org/sgp/crs/intel/RL33873.pdf ("Almost all assessments of the attacks of September 11, 2001, have concluded that U.S. intelligence and law enforcement agencies had failed to share information that might have provided advanced warning of the plot.").

officials. Specifically, subsection 203(b) of the PATRIOT Act amended Title III of the Wiretap Act to authorize law enforcement officers and Government attorneys to share "foreign intelligence" information obtained by Title III-authorized wiretap with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official."[115] Subsection 203(d) authorizes sharing of foreign intelligence information gathered during federal criminal investigations with the same types of federal officials.[116] Section 504 of the PATRIOT Act permits federal intelligence officers to consult with Federal and State law enforcement "to coordinate efforts to investigate or protect against" threats to national security.[117]

Sharing of foreign intelligence information among federal, state, and local law enforcement is also facilitated through state-run "fusions centers."[118] In 2003, the U.S. Department of Justice (DOJ) issued the National Criminal Intelligence Sharing Plan to emphasize the increased role of state and local law enforcement in domestic intelligence.[119] Based on this plan, DOJ and the U.S. Department of Homeland Security (DHS) issued federal guidelines for the establishment and operation of fusion centers in 2006.[120] The federal guidelines described "a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector."[121] Law enforcement agencies located in jurisdictions that currently operate fusion centers should follow existing protocol on information sharing with respect to UAS/UAV-gathered electronic data.

While some of the barriers separating the foreign intelligence and law enforcement communities have been torn down in recent years, the separation between domestic law enforcement and U.S. military operations remains strong. The Posse Comitatus Act outlaws the willful use of any part of the Armed Forces to execute the law unless expressly authorized by the Constitution or by an act of Congress.[122] Specifically, the Act provides:

---

[115] 18 USC § 2517(6).
[116] 50 USC § 3365
[117] 50 USC § 1806(k)(1)
[118] See Michael Price, National Security and Local Police, Brennan Center for Justice, available at http://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf.
[119] Global Info. Sharing Initiative, U.S. Dep't of Justice, The National Criminal Intelligence Sharing Plan (2003), available at http://www.au.af.mil/au/awc/awcgate/doj/nat_crim_intel_share_plan2003.pdf.
[120] Global Justice Info. Sharing Initiative, U.S. Dep't of Justice, et al., Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era 2 (2006) [hereinafter Fusion Center Guidelines], available at http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.
[121] Fusion Center Guidelines, at 29.
[122] *See* Charles Doyle & Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* Summary, Congressional Research Service (Aug. 16, 2012) (hereinafter, the "CRS Report"), *available at* http://www.fas.org/sgp/crs/natsec/R42659.pdf.

UAS Legal Memoranda, continued

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.[123]

Though the particular language of the Act mentions only the Army and the Air Force, Department of Defense policy has extended its application to all branches of the U.S. military.[124]

Questions concerning the Act's application arise most often in the context of assistance to civilian police.[125] At least in this context, the courts have held that, absent a recognized exception, the Posse Comitatus Act is violated when (1) civilian law enforcement officials make "direct active use" of military investigators; or (2) the use of the military "pervades the activities" of the civilian officials; or (3) the military is used so as to subject "citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature."[126] It is important to note that the Act is not violated when the Armed Forces conduct activities for a military purpose.[127]

One important exception relating specifically to information sharing was carved out by Congress in 1981. The 1981 exception, designed to promote military cooperation with criminal investigations of narcotics trafficking in the Caribbean,[128] provides that "[t]he Secretary of Defense may . . . provide . . . civilian law enforcement officials any information collected during the normal course of military training or operations."[129] Thus, Armed Forces can legally share information with domestic law enforcement if they just so happen to come across it in the ordinary course of business, by they *cannot* share information/intelligence they have deliberately set out to collect on law enforcement's behalf.[130]

---

[123] 18 U.S.C. § 1385.

[124] See Daniel Gonzalez et al, Improving Interagency Information Sharing Using Technology Demonstrations, The RAND Corporation (2014), available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR551/RAND_RR551.pdf.

[125] *See* Charles Doyle & Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* Summary, Congressional Research Service (Aug. 16, 2012) (hereinafter, the "CRS Report"), *available at* http://www.fas.org/sgp/crs/natsec/R42659.pdf.

[126] *Id.* at 54 and n.322. For an in depth discussion of exceptions, see the CRS Report at 29-51.

[127] *See id.* at 46-51.

[128] *See* Nathan Alexander Sales, Mending Walls: Information Sharing After the USA PATRIOT Act, 88 Tex. L. Rev. 1795, 1827 (2010) (citing Roger Blake Hohnsbeen, *Fourth Amendment and Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement*, 54 Geo. Wash. L. Rev. 404, 416-19 (1986)).

[129] 10 U.S.C. § 371(a).

[130] *See Sales* at 1827 and n. 210.

The 1981 exception does not directly address whether domestic law enforcement can legally share collected information with the Armed Forces. Therefore, the question becomes whether, in Posse Comitatus terms, the Armed Forces "execute the laws" when they use in military operations data that was gathered *via* UAV or UAS by domestic law enforcement for policing purposes. This kind of exchange is not clearly unlawful.[131] But while police may risk little harm from sharing UAV/UAS-gathered electronic data with Armed Forces, such a practice may make citizens uncomfortable.

A second important provision of federal law that restricts the use of U.S. military for law enforcement activities is found at Title 10, Section 375 of the U.S. Code:

> The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.[132]

This provision generally prohibits members of the U.S. military from directly participating in the search, seizure or arrest of a U.S. citizen or other person on U.S. territory unless specifically authorized by law.[133] Nevertheless, certain forms of indirect assistant from the U.S. military to domestic law enforcement may be permissible. Section 371 notably permits the military to share information collected during military operations and training with law enforcement when such information "may be relevant to a violation of any Federal or State law."[134]

VI. RECOMMENDED PRACTICES

As repeated throughout, no federal legislation explicitly regulates UAS/UAV-gathered electronic data and little in the way of state law exists on the topic. Existing federal legislation and legal principles can be used, by analogy, to create a piecemeal legal framework. Although this framework fails to provide truly meaningful or cohesive regulation, it does highlight a basic set of issues and concerns that law enforcement must address with respect to UAS/UAV data. The following guidelines are recommended practices for law enforcement to avoid legal pitfalls in UAS/UAS electronic data collection and use:

---

[131] Sales reaches the same conclusion. *See id.*

[132] 10 USC § 375.
[133] 10 USC § 375.
[134] 10 USC § 371.

UAS Legal Memoranda, continued

First, law enforcement must ensure that the collection of electronic data by UAS/UAV is conducted in a non-discriminatory manner and is reasonably limited in its scope. UAS/UAV must be lawfully present at the vantage point from which data is collected. Where the data collected includes audio-recordings of protected communications, officers must comply with Title III of the Wiretap Act regarding authorization, minimization, and providing notice of surveillance.

Second, law enforcement agencies that plan to retain any UAS/UAV-gathered electronic data must implement sufficient security and access controls. When necessary, officers must also comply with Title III requirements regarding sealing and storage of surveillance records.

Third, UAS/UAV-gathered data should be used and disclosed exclusively for law enforcement purposes, unless exigent circumstances warrant otherwise. Officers must recognize that disclosure of personal information can result in unlawful invasion of privacy and exercise significant care when accessing and sharing such data.

Fourth, to further transparency and public engagement, officials should disclose by way of publically-available, published guidelines specifically what happens to information once it is collected by UAS/UAV as well as how the collected information may or will be used.[135] Officials should specifically address:

- whether captured data is retained or discarded;
- if data is retained, officials should specify for how long data is retained and where it is retained, i.e., is a separate database maintained; is the data incorporated into other government databases?;
- what other government-controlled electronic databases the law enforcement agency compares captured data with (sex offenders, suspects wanted by police, etc.);
- and what actions the law enforcement agency takes when it detects a match.[136]

Fifth, law enforcement agencies must ensure that UAS/UAV surveillance policies are written and that they include sufficient accountability and transparency. The ABA Standards suggests that law enforcement officials should be held accountable for the use of physical surveillance technology by periodic review of the scope and effectiveness of the surveillance program.[137] The ABA Standards also suggest that accountability can be furthered by "[m]aintaining and making

[135] Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. Tech. L. & Pol'y 143, 171 (2004)
[136] Max Guirguis, Electronic Visual Surveillance and the Reasonable Expectation of Privacy, 9 J. Tech. L. & Pol'y 143, 171 (2004).
[137] ABA Standards, supra note 5.

available to the public general information about the type or types of surveillance being used and the frequency of their use."[138]

Public concern over potentially limitless surveillance capabilities of sophisticated UAS/UAV technology may stem from fear that officers will be watching and recording their every move. As noted by the International Association of Chiefs of Police (IACP) in the 2014 "IACP Technology Policy Framework", a "principal tenet of policing is the trust citizens grant police."[139] Law enforcement should take reasonable steps to dispel concerns and foster public trust in UAS/UAV programs in order to maximize the potential utility and public benefit offered by these emerging technologies.

[138] ABA Standards, supra note 5.
[139] *See* International Association of Chiefs of Police Aviation Committee, *Recommended Guidelines for the use of Unmanned Aircraft* (Aug. 2012), *available at* http://www.theiacp.org/portals/0/pdfs/iacp_uaguidelines.pdf.

SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Police Use of UAVs: Liability Analysis and Risk Management Considerations

TO: **The Police Foundation and the U.S. Department of Justice – COPS Office**

FROM: **Anne T. McKenna, Esquire**
Silverman|Thompson|Slutkin|White|LLC

DATE: **April 14, 2014; edited July 14, 2014**

RE: ***Community Policing and UAS Guidelines to Enhance Community Trust***
2013-CK-WX-K002
Police Use of UAVs: Liability Analysis and Risk Management Considerations

MEMORANDUM OVERVIEW

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between the Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled, *Community Policing and UAS Guidelines to Enhance Community Trust* (the "COPS contract"). Pursuant to the COPS contract Task 1 (detailed description of work appended to the COPS contract), this second memorandum ("Liability Analysis Memo") addresses Task 1's Line Item (7), which is a preliminary overview of liability concerns associated with police use of UASs/UAVs. This Memo is structured as follows:

I. POTENTIAL LIABILITY EXPOSURE

A. Overview of Law Enforcement Liability: General Principles
   i. Waiver of Federal and State Sovereign Immunity
   ii. Constitutional Torts

B. Specific UAV Incidents and Potential Liability Exposure
   i. UAV Collisions
   ii. Violation of Property Rights
   iii. Interference with Communications Systems
   iv. Violation of the Fourth Amendment and Right to Privacy
      1. Intrusion Upon Seclusion
      2. Constitutional Torts

   v. Liability Based on Federal Statute
      1. Title III – The Wiretap Act
      2. Pending Federal Legislation

II. RISK MANAGEMENT

A. UAS Program Training
B. UAS Program Operating Procedures
C. UAS Program Oversight

In sum, this Liability Analysis Memo provides a preliminary overview of liability concerns that should be addressed by any department or agency utilizing UAS, including risk management, risk avoidance, training, and potential civil and criminal liability exposure from the use of UAS. The Liability Analysis Memo also provides specific informative examples of how law enforcement has been deemed to be liable for use of certain electronic surveillance and other equipment, and how these principles of liability for equipment usage may provide guidance to potential liability for use of UAS/UAV equipment.

SUBJECT INTRODUCTION

Unmanned Aerial Vehicles (UAVs) offer numerous benefits to domestic law enforcement. However, the presence of UAVs in domestic airspace also poses risk of injury to persons, property, and civil rights. This risk of injury in turn creates a potential of civil liability for law enforcement agencies who utilize UAVs.

UAS Legal Memoranda, continued

The potential injuries and resulting liability caused by UAVs can be roughly divided into two categories:

(1) *injury to a person or his or her property* resulting from UAV collisions or other physical intrusions; and
(2) *injury to a person's right to privacy* resulting from UAV intrusion into his or her private space or affairs.

The first category is a familiar concept, similar to the liability that arises when a police officer negligently causes a car accident, or when a police helicopter collides with a private residence. The second category relates to the Fourth Amendment right to be free of unreasonable search and seizure. This right is asserted most often as a defense to criminal charges, *e.g.,* where a UAV employs a thermal-imaging device to determine heat patterns inside a private home. The Supreme Court has held that use of thermal imager in such a manner violates a homeowner's Fourth Amendment rights.[1] Thus, any resulting evidence from such a search would be suppressed, but more importantly for our analysis purposes in this Memo, the homeowner in question could initiate a civil rights and invasion of privacy lawsuit against the officer or agency to recover any damages that result.

In address both categories of potential liability (injury to person or property and injury to a person's right to privacy), This Liability Analysis Memo first provides a general overview of how and when law enforcement can be subject to civil lawsuits, followed by a discussion of specific incidents involving UAVs and the types of civil liability that could result. The final section offers risk management suggestions for law enforcement agencies with respect to training, operational procedures, and oversight of UAS programs.

I. POTENTIAL LIABILITY EXPOSURE

A. Overview of Law Enforcement Liability: General Principles and Causes of Action

i. Waiver of Federal and State Sovereign Immunity

Sovereign immunity traditionally protects federal and state governments from civil suit, but this immunity has largely been waived at both the federal and state levels. For example, the U.S. federal government, through the Federal Tort Claims Act, accepts liability for the negligent acts of government employees who are acting within the scope of their official employment duties.[2] This liability is imposed "in the same manner and to the same extent as a private

[1] *Kyllo v. United States*, 533 U.S. 27 (2001).
[2] 28 U.S.C. §§ 1346(b), 2671-80 (2006).

individual under like circumstances."[3] In addition, the cause of action must be one recognized by state law; the FTCA is merely a procedural statute and creates no substantive causes of action against the United States.

In general, a law enforcement officer is personally responsible for her own negligent or tortious acts, unless she can invoke an immunity defense. A police officer can generally claim immunity from tort liability when her acts are discretionary. A police officer also receives qualified immunity from civil rights liability when her acts did not violate a clearly established statutory or constitutional right. Immunity defenses are generally not available where a police officer commits an intentional tort.[4] Both the police officer and the employing government agency can be held jointly and severally liable for the victim's injuries based on the doctrine of *respondeat superior*.[5]

ii. "Constitutional Torts"

A party who believes her Fourth Amendment rights have been violated by law enforcement can file a civil rights lawsuit based on 42 U.S.C § 1983. Section 1983 permits federal suit against local governments and state and local government employees based on violation of a federal constitutional or statutory right. This statute creates a private cause of action against any "person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws."[6] The Supreme Court expanded this liability to include municipalities, but only "when execution of a government's policy or custom…inflicts the injury."[7]

An individual could also bring a "*Bivens* Action," which is a claim for damages against federal officials for violating that person's constitutional rights. The absence of a statute granting the right to recover damages does not prevent such suits.[8] A *Bivens* claim can be maintained against federal officers only in their individual capacities.[9] A claim against federal officers in their official capacities requires a waiver of sovereign immunity.[10]

---

[3] 28 U.S.C. § 2674.
[4] *See* Eugene McQuillin, *The Law of Municipal Corporations* §45:52 (3d ed. 2006).
[5] *Respondeat Superior* is a latin phrase, meaning in common parlance: "Let the chief answer." A superior is responsible for any acts of omission or commission by a person of less responsibility to him. http://thelawdictionary.org/respondeat-superior/
[6] 42 U.S.C.A. § 1983.
[7] *Monell v. Dep't of Soc. Servs. of City of New York*, 436 U.S. 658, 694, 98 S. Ct. 2018, 2037-38, 56 L. Ed. 2d 611 (1978).
[8] *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).
[9] *Nurse v. United States*, 226 F.3d 996, 1004 (9th Cir. 2000).
[10] *Id.*

UAS Legal Memoranda, continued

Government officials may be entitled to qualified immunity where "their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[11] The availability of qualified immunity is measured by "the 'objective legal reasonableness' of the action, assessed in light of the legal rules that were 'clearly established' at the time the action was taken."[12]

B. Specific UAV Incidents and Potential Liability Exposure

i. UAV Collisions

Recent incidents of UAV crashes have been well-documented by the media.[13] When a UAV or its component parts crashes to the ground, both property loss and human casualties can occur. Another risk associated with UAVs flying in domestic airspace is in-air collisions with other aircraft, including passenger airplanes and other UAVs.

Due to the relatively recent emergence of law enforcement use of UAVs, legal rules directly related to civil liability in this context are sparse. Legal rules regarding government-operated aircraft and motor vehicles are instructive by analogy with respect to personal injury and property damages caused by UAV crashes.

Aircraft collisions resulting in ground damage can give rise to civil liability based on claims of either negligence or strict liability.[14] In its early years, aviation was considered an "ultrahazardous activity" by the legal community. Those who engage in such an activity are strictly liable for any resulting damage, regardless of how much or how little care they exercised. As aircraft operation became safer and more widespread, many courts shifted toward imposing liability only where there was negligence on behalf of the operators and owners of damage-causing aircraft, rather than holding them strictly liable.[15]

In states that continue to apply strict liability to ground damages resulting from aircraft accidents, whether this standard applies to UAV accidents may depend on whether a "unmanned aerial *vehicle*" is deemed to be an "aircraft."[16] However, a court may apply strict liability regardless where it deems the operation of UAVs to be an abnormally dangerous activity subject

---

[11] *Harlow v. Fitzgerald*, 457 U.S. 800, 818, 102 S. Ct. 2727, 2738, 73 L. Ed. 2d 396 (1982).
[12] *Anderson v. Creighton*, 483 U.S. 635, 107 S. Ct. 3034, 3036, 97 L. Ed. 2d 523 (1987) (*quoting Harlow v. Fitzgerald*, 457 U.S. 800, 102 S.Ct. 2727, 73 L.Ed.2d 396).
[13] Chris Lawrence, *Navy Drone Crashes in Maryland*, CNN, June 11, 2012, *available at* http://www.cnn.com/2012/06/11/us/maryland-drone-crash; Military Drone Crashes Near Pennsylvania Elementary School, RT.com, April 5, 2014, *available at* http://rt.com/usa/military-drone-crashes-pa-school-501/.
[14] 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, 635 (2009).
[15] *Id* at 636.
[16] *Id.*

to strict liability.[17] Where strict liability does not apply to ground damages resulting from UAV collisions, injured parties could bring claims against law enforcement alleging negligent operation or maintenance of the UAV.

Negligent operation and maintenance are also viable causes of action to recover damages caused by in-flight collisions. Negligent piloting of manned aircraft focuses largely on a pilot's duty to "see and avoid" airspace traffic. It is presently unclear what constitutes reasonable care and watchfulness during the in-flight operation of UAVs; thus, what degree of carelessness gives rise to civil liability for negligent operation remains to be seen.

ii. Violation of Property Rights

Low-flying UAVs may give rise to a landowner's claim for both trespass and nuisance.[18]

UAVs flying above an individual's property may create noise pollution or visual pollution. If such pollution arises to "a substantial and unreasonable interference" with the "use and enjoyment" of property, it could support a private nuisance claim against the responsible law enforcement agency or municipality. Landowners have succeeded in nuisance claims against municipalities based on noise pollution created by aircraft. The altitude of an aircraft is a key factor to finding whether the noise pollution constitutes actionable nuisance.

Landowners have also successfully brought trespass claims based on low-flying aircraft, but only where such low-level flights have actually interfered with the owner's use of the land.

iii. Interference with Communications Systems

UAS operation that depends on communications connections can create harmful interference with communication systems in several ways. UAS communication signals could interfere with cell phone, internet or television signals. Members of the public or service providers who suffer damages as a result of this service loss could seek compensation from the law enforcement agency whose UAS operation caused the interference.[19]

Conversely, interruption of UAS communication systems could also give rise to civil liability. Signals between the UAV and its operator could be disrupted, potentially causing an air-to-air or ground collision that could give rise to liability for resulting damages.[20] A UAS could also be hacked by a third party. The UAV itself could be used by the hacker to injure persons or property, or the hacker could gain unauthorized access to the surveillance records

[17] *Id* at 637.
[18] *Great Westchester Homeowners Assn' v. City of Los Angeles*, 603 P.2d 1329 (Cal. 1979).
[19] Rapp, *supra* note 12, at 630.
[20] *Id* at 630.

UAS Legal Memoranda, continued

collected by the UAS.[21] If a law enforcement agency is negligent in safeguarding against such risks, it could be held liable for resulting injuries. For example, municipal liability was upheld in a wrongful death action where a police officer negligently permitted his vehicle to be stolen by an escaped prisoner, and that prisoner caused a collision resulting in the death of a civilian.[22]

iv. Violation of the Fourth Amendment and Right to Privacy

UAV surveillance by law enforcement may give rise to claims related to invasion of privacy or violation of the Fourth Amendment. This discussion identifies how a citizen may seek redress of a constitutional violation; whether certain UAV usage constitutes a violation is addressed in Legal Memo 1. While such claims will most likely arise primarily in defense of criminal charges, it may be possible for UAV surveillance to constitute grounds for a civil action. For example, an individual may claim that such surveillance constitutes a common law tort of intrusion upon seclusion, or a "constitutional tort" due to violations of Fourth Amendment rights against unreasonable search and seizure. However, a plaintiff must prove "actual injury" to recover damages pursuant to either type of claim.[23]

1. Intrusion Upon Seclusion

An individual who seeks to recover damages based on the common law action for intrusion upon seclusion must show that the claimed intrusion is upon his "solitude or seclusion…or his private affairs or concerns" and is "highly offensive to a reasonable person."[24] Thus, if a UAV captures photograph or visual images of the plaintiff without his consent and within his private home, that person may recover damages for intrusion upon seclusion if he suffered emotional distress or other injuries.[25]

2. "Constitutional Torts"

A party who believes her Fourth Amendment rights have been violated by law enforcement can file a civil rights lawsuit based on 42 U.S.C § 1983. This statute creates a private cause of action against any "person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and

[21] *Id* at 362.
[22] *Finnigan v. Blanco County*, 670 S.W.2d 313 (Tex. App. 1984).
[23] See *Memphis Comm. Sch. Dist. v. Stachura*, 477 U.S. 299, 308 (1986).
[24] Restatement (Second) of Torts § 652B (1977).
[25] See Brian Craig, *Online Satellite and Aerial Images: Issues and Analysis*, N.D. L. Rev. 547, 562 (2007).

laws."[26] An individual could also bring a "*Bivens* Action," which is a claim for damages against federal officials for violating that person's constitutional rights.[27]

Where a UAV obtains imagery of an individual in violation of the Fourth Amendment and that individual is able to prove "actual injury" as a result, he may be able to recover resulting damages from law enforcement through either a section 1983 or a "*Bivens* Action." Unlawful electronic surveillance may give rise to liability under section 1983.[28] An individual may be able to prove "actual injury" where these images are made public, even if unintentionally or through third-party interception.[29] For example, the 11th Circuit upheld a § 1983 claim when it determined that officers violated the constitutional right to privacy when an officer seized a video tape of the plaintiff engaging in sexual acts and then circulated the tape among other officers.[30] However, law enforcement may be entitled to qualified immunity based on a lack of clearly established legal rules governing the Fourth Amendment implications with respect to UAV surveillance.

v. Liability Based on Federal Statute

In addition to lawsuits based on state law and "constitutional tort" claims, plaintiffs can also bring suit against law enforcement agencies based on federal statutes that authorize private causes of action. In particular, federal law that prohibits unauthorized wiretapping permits a party subjected to prohibited wiretapping to file a civil lawsuit against the party who violated this law. Law enforcement use of UAVs that employ audio-recording technology could potentially engage in such unauthorized wiretapping, and thus be subject to civil liability. The following discussion simply highlights one of many federal laws that could potentially be a basis for civil liability; violation of other federal and state statutes may also create exposure to lawsuits.

1. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (The "Wiretap Act")

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the "Wiretap Act" prohibits the unauthorized, nonconsensual interception of "wire, oral, or electronic communications."[31] Section 2520 of the Act states that "any person whose wire, oral,

[26] 42 U.S.C.A. § 1983.
[27] *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).
[28] *Police Misconduct: Law and Litigation* § 2:24. In *Whitaker v. Garcetti*, 291 F. Supp. 2d 1132 (C.D. Cal. 2003), aff'd in part, vacated in part, rev'd in part, 486 F.3d 572, 67 Fed. R. Serv. 3d 1167 (9th Cir. 2007), the district court was presented with a § 1983 claim based on undisclosed use of wiretapping obtained in violation of the Fourth Amendment. The district court concluded that the wiretapping scheme was per se unconstitutional. However, both the district court and the Ninth Circuit determined that the subjects of the search were barred from bringing a § 1983 claim because they had been convicted of criminal offenses that had not been reversed or vacated.
[29] Rapp, *supra* note 12, at 643.
[30] *James v. City of Douglas, Ga*., 941 F.2d 1539 (11th Cir. 1991).
[31] 18 U.S.C. § 2511.

UAS Legal Memoranda, continued

or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation."[32] The Act does not define what constitutes an "entity" and courts have split over whether state and local government agencies qualify as such. Several courts have held that state government agencies can be sued for the unlawful interception, disclosure or use of communications under § 2520. However, other courts have held that Congress did not intend for local government agencies to be considered an "entity" susceptible to civil liability under § 2520.[33] It is also important to note that while video surveillance is not explicitly included within the scope of Title III, the Act's requirements and prohibitions may nevertheless be triggered where the video technology also captures audio recordings or oral or wire communications.

Civil liability can also arise where intercepted communications are wrongfully disclosed: *(g) Improper disclosure is violation.*—Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).[34]

Recall that in *Katz v. United States*, the Supreme Court emphasized that the Fourth Amendment "protects people, not places."[35] Subsequently, what a person "seeks to keep private, even in an area accessible to the public, may be constitutionally protected."[36] Thus, private conversations taking place in public may still be afforded Title III protection against unlawful interception. Where UAV surveillance by law enforcement results in the unauthorized and non-consensual interception of in-person or cell phone conversations intended to be private, civil liability under Title III may arise.

2. *Pending Federal and State Legislation Specifically Regulating UAV/UAS*

Several bills pending before Congress aim to regulate the use of UAVs in domestic surveillance operations. A number of these proposals would create private rights to sue for violations of that legislation. The Preserving Freedom from Unwarranted Surveillance Act of 2013 (H.R. 972) would create a right to sue for any violation of its prohibitions[37]. H.R. 1262, The Drone Aircraft Privacy and Transparency Act of 2013 (H.R. 1262) would provide for a private right of action for a person injured by a violation of this legislation.[38] In addition, the Preserving American Privacy Act of 2013 (H.R. 637) would permit administrative discipline

[32] 18 U.S.C. § 2520.
[33] *See* Fishman and McKenna, *Wiretapping and Eavesdropping* § 3:42.
[34] 18 U.S.C. § 2520(g); *see generally,* Fishman and McKenna, *Wiretapping and Eavesdropping* § 3:40.
[35] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[36] *Id* at 351.
[37] H.R. 972, 113th Cong. (1st Sess. 2013).
[38] H.R. 1262, 113th Cong. (2d Sess. 2013).

against an officer who intentionally violates a provision of the act.[39] Law enforcement agencies seeking to implement UAV programs should keep abreast of legislative developments, as this issue has received increased Congressional attention.

Numerous states have passed legislation that regulate the use of UAVs by both police and private individuals and businesses. It is essential that any police department that employs a UAS/UAV ensures prior to use that its actions comport with state law.

II. RISK MANAGEMENT

UAS operation by law enforcement agencies in public spaces poses a variety of safety risks and potential exposure to legal liability. In addition, the unique capabilities of this powerful technology make it particularly susceptible to potential abuse.[40] It is essential that any law enforcement agency considering usage of UAS implement standard operating procedures that are applied uniformly and followed consistently. Agencies must also ensure that every UAS deployment obtains and strictly adheres to the Certificate of Authorization (COA) issued by the Federal Aviation Administration (FAA).

For an excellent example of UAS operating procedures, see *Special Operations Standard Operating Procedures, Arlington, Texas Police Department*. The standard operating procedures developed by Arlington Texas Police Department for its small Unmanned Aircraft System (Arlington-TX UAS SOP) program presents a comprehensive policy "designed to minimize risk to people, property, and aircraft during the operations of the sUAS while continuing to safeguard the right to privacy of all persons."

We have reviewed closely the Arlington-TX UAS SOP. It is our legal opinion that this SOP is an excellent model for a proposed uniform UAS-SOP for any police department.

A. UAS Program Training

Law enforcement officers involved in the use of UAS must be properly trained with respect to the operation of that UAS, ideally by representatives of the manufacturer or certified instructors. Additional specialized training may be necessary for certain specific missions. Officers performing specific functions during the UAS operation, such as the camera operator or flight observer, will also require additional specialized training. Officers piloting the UAS must ensure they possess proper certifications as required by the FAA.

---

[39] H.R. 637, 113th Cong. (1st Sess. 2013).
[40] See Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 Mich. Telecomm. & Tech. L. Rev. 589, 610 (2012) (citing Associated Press report on New York City police officers using surveillance cameras to "take pictures up women's skirts or down their blouses on city streets.")

UAS Legal Memoranda, continued

In addition to mastering the logistical operations of UAS, officers involved in UAS missions must have a thorough understanding of Fourth Amendment law, as discussed in Legal Memo 1. Officers must recognize UAS activities that violate a civilian's constitutional rights, and officers must know how and when to avoid such violations. It is particularly important that officers recognize when their conduct approaches a potential or uncertain violation, as the parameters of Fourth Amendment protections are imprecise and constantly evolving. Without a strong grasp of Fourth Amendment jurisprudence, law enforcement agencies will be at heightened risk of incurring major civil liability and jeopardizing ongoing criminal investigations.

B. UAS Program Operating Procedures

Law enforcement agencies must develop detailed procedures for every stage of UAS operation. Agencies must ensure that UAS are properly maintained, which should include pre-flight and post-flight inspections. Agency policy should also require detailed reporting and documentation of all maintenance performed, any equipment issues encountered, and any changes to the UAS software or hardware.

Prior to flight, agencies should review the goals and scope of the mission, the role to be played by the UAS in that mission, the flight area, weather conditions, and any other issues that will inform UAS operation. Advance notice of all training and mission operations must be provided to air traffic control and any other parties as required by local aviation authorities. Agencies should also develop procedures to follow in the event of loss of communications signal or visual contact with the UAV, UAV collision, or other emergency events.

In-flight operational procedures should include measures to avoid collision with other aircraft and property, and steps to take when risk of harm arises. Agencies should also clearly identify prohibited acts involving UAS and ensure that all officers involved in UAS operations recognize and understand when there is a risk that a prohibited act may occur. Such prohibited acts should include warrantless searches, outfitting UAVs with weaponry. In general, operational procedures should discourage the use of UAS where the risks of deploying the UAS outweigh the benefit to the law enforcement mission.

C. UAS Program Oversight

Any UAS program must include procedures for auditing, a system of oversight, and consequences for abuse. UAS technology is highly susceptible to misuse, and such misuse can create significant civil – and possibly criminal – liability for officers, supervisors, and state and local government entities. Due to the serious risks involved, law enforcement agencies should

ensure that an adequate system of checks and balances is in place to prevent the possibility of systematic abuse.

Overview of UAS/UAV-Related State Legislation

SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Overview of UAS/UAV-Related State Legislation

TO: The Police Foundation and the U.S. Department of Justice – COPS Office

FROM: Anne T. McKenna, Esquire

DATE: May 22, 2014; final edits July 31, 2014

RE: *Community Policing and UAS Guidelines to Enhance Community Trust*

2013-CK-WX-K002

State Legislation Related to UAVs

OVERVIEW

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between the Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled, *Community Policing and UAS Guidelines to Enhance Community Trust* (the "COPS Contract"). Pursuant to the COPS Contract Task 1 (detailed description of work appended to the COPS Contract) Line Item (4) and as discussed with the Police Foundation's Grants Manager, Maria Valdovinos, this legal memorandum consists of the attached reference chart of the currently enacted state laws pertaining to or proscribing the use of UAS.

1

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Alabama	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Alaska	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Arizona	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Arkansas	No Currently Enacted Legislation, but Legislation Proposed or Pending						
California	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Colorado	No Currently Enacted or Proposed/Pending Legislation						

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Connecticut	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Delaware	No Currently Enacted or Proposed/Pending Legislation						
District of Columbia	No Currently Enacted or Proposed/Pending Legislation						
Florida	SB 92 (Freedom from Unwanted Surveillance Act) Statutory Cite: Searches and Seizure Using a Drone, FL ST § 934.50	Police ONLY	YES	YES	• Generally prohibits law enforcement to use "drones" to "gather evidence or other information" • EXCEPTIONS: o To counter a high risk of a terrorist attack if the U.S. Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk o Warrant o Reasonable suspicion that swift action is needed to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect or the destruction of evidence, or to achieve purposes including, but not limited to, searching for a missing person • DEFINITIONS: o Drone = a powered aerial vehicle that doe s not carry a human operator, uses	YES "An aggrieved person may initiate a civil action against a law enforcement agency to obtain all appropriate relief in order to prevent or remedy a violation"	• ADMISSIBILITY: Evidence obtained or collected in violation of the law is not admissible as evidence in a criminal prosecution in any court of law in the state. No regulation of retention or disclosure

3

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload ○ Law enforcement agency = a lawfully established state or local public agency that is responsible for the prevention and detection of crime, local government code enforcement, and the enforcement of penal, traffic, regulatory, game, or controlled substance law		
Georgia	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Hawaii	SB 1121	N/A	N/A	N/A	• Appropriates $100,000 for fiscal year 2013-2014 for a Program Coordinator and technical support staff member for the proposed international flight training center and associated degree programs at the University of Hawaii at Hilo and Hawaii Community College.	N/A	N/A
	Other Legislation is Proposed or Pending						
Idaho	SB 1134 Statutory Cite: Restrictions on use of	Police AND Private Persons	YES	YES	• Prohibits the use of UAS to "intentionally conduct surveillance of, gather evidence or collect information about, or photographically or electronically record specifically targeted	YES Recovery of the greater of $1,000 or	No regulation of retention, disclosure, or admissibility

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
	unmanned aircraft systems, ID ST § 21-213				persons or specifically targeted private property" • EXCEPTIONS: ○ Warrant ○ Emergency response for safety ○ Search and rescue investigations ○ Controlled substance investigations • Also prohibits the use of UAS to "photograph or otherwise record an individual, without such individual's written consent, for the purpose of publishing or otherwise publicly disseminated such photograph or recording • DEFINITIONS: ○ Unmanned aircraft system (UAS) = an unmanned aircraft vehicle, drone, remotely piloted vehicle, remotely piloted aircraft or remotely operated aircraft that is a powered aerial vehicle that does not carry a human operator, can fly autonomously or remotely and can be expendable or recoverable; specifically DOES NOT include model flying airplanes or rockets and unmanned aircraft systems used in mapping or resource management • Creates civil cause of action for violation	actual and general damages, plus reasonable attorney's fees and costs	
	Other Legislation is Proposed or Pending						

5

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Illinois	SB 1587 (Freedom from Drone Surveillance Act) Statutory Cite: IL ST CH 725 § 167/1, *et seq.*	Police ONLY	YES	YES	• Generally prohibits use of a "drone" to "gather information" • EXCEPTIONS: ○ To counter a high risk of a terrorist attack if the U.S. Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk ○ Warrant (based on probable cause) limited to 45 days ○ Reasonable suspicion that swift action is needed to prevent imminent harm to life, or to forestall the imminent escape of a suspect or the destruction of evidence (use limited to 48 hours, and within 24 hours of initiation of use, chief executive officer of the law enforcement agency must report the use to the local State's Attorney in writing) ○ Attempts to locate a missing person, not in relation to a criminal investigation ○ Crime scene and traffic crash scene photography in "a geographically confined and time-limited manner" and if on private property requires either a search warrant or lawful consent to search • DEFINITIONS: ○ Drone = any aerial vehicle that does not carry a human operator ○ Information = any evidence, images, sounds, data, or other information gathered by a drone ○ Law enforcement agency = any agency of this State or a political subdivision of this State which is vested by law with the duty to maintain public order and to enforce criminal laws	NO	• RETENTION: Info gathered by a drone must be destroyed by the agency within 30 days EXCEPT a supervisor at the agency may retain particular information if there is reasonable suspicion that the information contains evidence of criminal activity or the information is relevant to an ongoing investigation or pending criminal trial • DISCLOSURE: Disclosure of info gathered by a drone may not be disclosed EXCEPT a supervisor of the agency may disclose particular information to another government agency if there is reasonable suspicion that the information contains evidence of criminal activity or the information is relevant to an ongoing investigation or pending criminal trial • ADMISSIBILITY: If a court finds by a preponderance of the evidence that police used a drone to gather information in violation of the law, the information shall be presumed to be inadmissible in any judicial or administrative proceeding. The State may overcome this presumption by proving the applicability of a judicially recognized exception to the exclusionary rule.

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
	HB 1652	Police AND Private Persons	N/A	N/A	• Criminalizes the intentional or knowing use of a drone to interfere with hunters or fisherman • DEFINITIONS: ○ Drone = any aerial vehicle that does not carry a human operator • Creates a civil cause of action for violation	YES Permits injunctive relief and award of all resulting costs and damages to a person adversely affected by a violation of the law, including an award of punitive damages	No regulation of retention, disclosure, or admissibility
	Other Legislation is Proposed or Pending						
Indiana	HB 1009 Statutory Cite: IC § 35-33-5-9(a); IN ST § 35-33-5-9(a); IC § 35-31.5-2-342.3	Police ONLY	YES	YES	• Generally requires a search warrant in order to use a UAV • EXCEPTIONS: ○ Exigent circumstances necessitating a warrantless search ○ Substantial likelihood of a terrorist attack ○ Search and rescue or recovery operation ○ Responding to or mitigating results of a natural disaster, or any other disaster ○ Performing a geographical, environmental, or other survey for a non-criminal justice purpose ○ Consent of affected property owner(s) • DEFINITIONS: ○ UAV = an aircraft that does not carry a human operator and is capable of flight under remote control or autonomous programming ○ Use of a UAV = the use of a UAV by police	NO	• ADMISSIBILITY: Communications or images obtained via UAV, and evidence derived therefrom, in violation of the law are not admissible as evidence in administrative or judicial proceedings No regulation of retention or disclosure

7

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					to obtain evidence relevant to the enforcement of statutes, rules, or regulations, including the interception of wire, electronic, or oral communications and the capture, collection, monitoring, or viewing of images ○ "Tracking device" is defined to include a UAV		
	Other Legislation is Proposed or Pending						
Iowa	*HF 2289* Statutory Cite: Use of unmanned aerial vehicle--prohibition--traffic law enforcement, IA ST § 321.492B	Police ONLY	N/A	N/A	• Prohibits the use of a UAV for traffic law enforcement	N	• ADMISSIBILITY: Information obtained by UAV is not admissible as evidence in a criminal or civil proceeding UNLESS the information is obtained pursuant to the authority of a search warrant or is otherwise obtained in a manner consistent with state and federal law No regulation of retention or disclosure
	Other Legislation is Proposed or Pending						
Kansas	No Currently Enacted Legislation, but Legislation Proposed or Pending						

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Kentucky	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Louisiana	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Maine	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Maryland	HB 0100/CH 0423	N/A	N/A	N/A	• Appropriates $500,000 to supplement the appropriation for fiscal year 2013 to provide funds to complete the proposal to operate an Unmanned Aerial Systems test site in the State	N/A	N/A
	Other Legislation is Proposed or Pending						
Massachusetts	No Currently Enacted Legislation, but Legislation Proposed or Pending						

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Michigan	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Minnesota	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Mississippi	No Currently Enacted or Proposed/Pending Legislation						
Missouri	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Montana	SB 196 Statutory Cite: MT ST § 46-5-109	Police AND Private Persons	N/A	N/A	• Generally prohibits using information obtained *via* UAV as evidence in any prosecution or proceeding within the State, subject to certain exceptions • EXCEPTIONS: ○ Warrant ○ In accordance with judicially recognized exceptions to the warrant requirement • Also prohibits use of information obtained *via* UAV in an affidavit of probable cause to obtain a search warrant UNLESS the information was obtained pursuant to a search warrant, in accordance with a judicially	N/A	• ADMISSIBILITY: Information from a UAV is not admissible as evidence in any prosecution or proceeding within the State UNLESS the information was obtained pursuant to the authority of a search warrant or in accordance with a judicially recognized exception to the warrant requirement

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					recognized exception to the warrant requirement, or through the monitoring of public lands or international borders • DEFINITIONS: ○ UAV = an aircraft that is operated without direct human intervention from on or within the aircraft and does not include satellites		
	Other Legislation is Proposed or Pending						
Nebraska	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Nevada	AB 507	N/A	N/A	N/A	• Appropriates $4,000,000 from the State General Fund to the Interim Finance Committee for allocation to the Governor's Office of Economic Development for the UAV program, but the money can only be allocated by the Interim Finance Committee if and when Nevada is selected as a FAA test site and submission by the Governor's Office of Economic Development of a plan for utilization of the funding including an analysis of the program's estimated impact and effectiveness	N/A	N/A
	Other Legislation is Proposed or Pending						

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
New Hampshire	No Currently Enacted Legislation, but Legislation Proposed or Pending						
New Jersey	No Currently Enacted Legislation, but Legislation Proposed or Pending						
New Mexico	No Currently Enacted Legislation, but Legislation Proposed or Pending						
New York	No Currently Enacted Legislation, but Legislation Proposed or Pending						
North Carolina	SB 402 (Appropriations Act of 2013) at § 7.16(e)	Police ONLY	N/A	N/A	• Until July 1, 2015, prohibits procuring or operating a UAS and/or disclosure of personal information about any person acquired *via* UAS UNLESS the State CIO approves an exception specifically allowing disclosure, use, and/or purchase • DEFINITIONS: ○ Unmanned aircraft = an aircraft that is operated without the possibility of human intervention from within or on the aircraft ○ UAS = an unmanned aircraft and associated elements, including	N/A	N/A

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					communication links and components that control the unmanned aircraft that are required for the pilot in command to operate safely and efficiently in the national airspace system		
	Other Legislation is Proposed or Pending						
North Dakota	SB 2018	N/A	N/A	N/A	• Appropriates $1,000,000 from the State general fund for costs related to pursuing designation as a FAA UAS test site. If selected by the FAA as a national test site, appropriates an additional $4,000,000 from the State strategic investment and improvements fund to operate the site.	N/A	N/A
	Other Legislation is Proposed or Pending						
Ohio	HB 497	N/A	N/A	N/A	• Appropriates $4,000,000 to fund the National Unmanned Aerial System Training Center and $350,000 to fund the UAS Verification/ Validation Testing Center, both at Sinclair Community College	N/A	N/A
	Other Legislation is Proposed or Pending						
Oklahoma	No Currently Enacted Legislation, but Legislation Proposed or Pending						

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Oregon	HB 2710 Statutory Cite: O.R.S. § 837.300(1).	Police AND Public Bodies[1]	YES	YES	• Generally prohibits police from operating a drone, acquiring information through the operation of a drone, and/or disclosing information acquired through the operation of a drone • EXCEPTIONS: ○ Warrant, limited to 30 days ○ Existence of probable cause to believe that a person has committed, is committing, or is about to commit a crime AND exigent circumstances exist making it unreasonable to obtain a warrant ○ To acquire information about an individual or the individual's property IF the individual has given written consent to the use of a drone for those purposes ○ For search and rescue activities, as defined in ORS 404.200 ○ To assist an individual in an emergency IF police believe there is an imminent threat to the life or safety of the individual and documents the factual basis for that belief (within 48 hours after the emergency operation begins, police official must file a sworn statement with the circuit court describing the nature of the emergency and the need for use of a drone) ○ During a state of emergency as declared by the Governor under ORS chapter 401	YES Prevailing plaintiff may recover treble damages for any injury to the person or property due to trespass by a drone, may be awarded injunctive relief, and may recover attorney's fees IF the amount pleaded is $10,000 or less	• ADMISSIBILITY: Generally, any image or other information acquired *via* drone by police in violation of this law, and any evidence derived from that image or information, is not admissible in, and may not be disclosed in, a judicial, administrative, arbitration, or other adjudicatory proceeding AND may not be used to establish reasonable suspicion or probable cause to believe that an offense has been committed. Specifically, any image or other information acquired *via* drone by police during training as permitted by this law, and any evidence derived from that image or information, is not admissible in, and may not be disclosed in, a judicial, administrative, arbitration, or other adjudicatory proceeding AND may not be used to establish reasonable suspicion or probable cause to believe that an offense has been committed. • ADMISSIBILITY: Until January 1, 2016, any image or other information acquired by a public body *via* a drone that has not been approved by the FAA, and any evidence derived from that image or information, is not

[1] "Public body" is defined as "state government bodies, local government bodies, and special government bodies" and includes every state officer, agency, department, bureau, board and commission; every county and city governing body, school district, special district, municipal corporation or any board, department, commission, council or agency thereof.

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					AS LONG AS the drone is used only for the purposes of preserving public safety, protecting property or conducting surveillance for the assessment and evaluation of environmental or weather-related damage, erosion, or contamination AND the drone is operated only in the geographical area specified in a proclamation pursuant to ORS 401.165(5) ○ To reconstruct a specific crime scene, or similar physical assessment, related to a specific criminal investigation, but only for 5 days ○ Training purposes • DEFINITIONS: ○ Drone = an unmanned flying machine, not including a model aircraft • Requires public bodies to register drones with the Oregon Department of Aviation, subject to a civil penalty of up to $10,000 • Prohibits use of weaponized drones by public bodies • Creates a civil cause of action for a person who owns or lawfully occupies real property in the state against a person or public body that operates a drone that is flown at a height of less than 400 feet over the property IF the operator of the drone has done so on at least one previous occasion and the person gave notice that he/she didn't want the drone flown over the property at a height of less than 400 feet		admissible in, and may not be disclosed in, a judicial, administrative, arbitration, or other adjudicatory proceeding AND may not be used to establish reasonable suspicion or probable cause to believe that an offense has been committed. No regulation of retention or disclosure

15

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					• EXCEPTIONS: ○ The drone is lawfully in the flight path for landing at an airport, airfield, or runway, AND ○ The drone is in the process of taking off or landing		
	Other Legislation is Proposed or Pending						
Pennsylvania	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Puerto Rico	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Rhode Island	No Currently Enacted Legislation, but Legislation Proposed or Pending						
South Carolina	No Currently Enacted Legislation, but Legislation Proposed or Pending						
South Dakota	No Currently Enacted or Proposed/Pending Legislation						

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Tennessee	SB 796 (Freedom from Unwanted Surveillance Act) Statutory Cite: T. C. A. § 39-13-609.	Police ONLY	YES	YES	• Generally prohibits use of a drone "to gather evidence or other information" • EXCEPTIONS: ○ To counter a high risk of a terrorist attack IF the U.S. secretary of homeland security determines that credible intelligence indicates that there is such a risk ○ Warrant ○ Reasonable suspicion that swift action is needed to prevent imminent danger to life • DEFINITIONS: ○ Drone = a powered aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload ○ Law enforcement agency = a lawfully established state or local public agency that is responsible for the prevention and detection of crime, local government code enforcement, and the enforcement of penal, traffic, regulatory, game, or controlled substance laws	YES	• ADMISSIBILITY: Evidence obtained or collected in violation of this law is not admissible as evidence in a criminal prosecution in any court of law in the state No regulation of retention or disclosure
	HB 1952 and SB 1777	Police AND Private Persons	N/A	N/A	• Prohibits anyone from using a drone to conduct video surveillance of private citizens who are lawfully hunting or fishing	NO	No regulation of retention, disclosure, or admissibility

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
	Other Legislation is Proposed or Pending						
Texas	HB 912 (Texas Privacy Act) Statutory Cite: V.T.C.A., Government Code § 423.001, *et seq.*, Use of Unmanned Aircraft.	Police AND Private Persons	YES	YES	• It is lawful to capture an image using an unmanned aircraft in the following 19 enumerated circumstances: ○ For purposes of professional or scholarly research and development by a person acting on behalf of an institution of higher education ○ In airspace designated as a test site or range authorized by the FAA for the purpose of integrated UAS into the national airspace ○ As part of an operation, exercise, or mission of any branch of the U.S. military ○ By a satellite for the purposes of mapping ○ By or for an electric or natural gas utility in certain enumerated circumstances ○ With the consent of the individual who owns or lawfully occupies the real property captured in the image ○ Warrant ○ By police (or a person under contract or otherwise acting under the direction of or on behalf of police)… ▪ In immediate pursuit of a person officers have reasonable suspicion or probable cause to suspect has committed an offense, not including misdemeanors or offenses punishable by fine only	YES Permits injunctive relief, recovery of a civil penalty of $5,000 for all images captured in a single violation or $10,000 for disclosure, display, distribution, or other use of any images captured in a single violation, or recovery of actual damages if the person who violated the law discloses, displays, or distributes the image(s) with malice (as defined in § 41.001 of the Civil Practice and Remedies Code), and awards court costs and reasonable attorney's fees to the prevailing party	• ADMISSIBILITY: An image captured in violation of the law, 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, BUT may be disclosed and used as evidence to prove violation of this law and is subject to discovery, subpoena, or other means of legal compulsion for that purpose • REPORTING: Creates reporting requirements for police No regulation of retention or disclosure

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					▪ To document a crime scene where an offense, not including misdemeanors or offenses punishable by fine only, has been committed ▪ To investigate the scene of a human fatality, a motor vehicle accident causing death or serious bodily injury to a person, or any motor vehicle accident on a state highway or federal interstate or highway ▪ In searching for a missing person ▪ To conduct a high-risk tactical operation that poses a threat to human life ▪ Of private property that is generally open to the public where the property owner consents to police public safety responsibilities ○ By police (or a person under contract or otherwise acting under the direction of or on behalf of police)… ▪ To survey the scene of a catastrophe or other damage to determine whether a state of emergency should be declared ▪ To preserve public safety, protect property, or survey damage or contamination during a lawfully declared state of emergency ▪ Conducting routine air quality sampling and monitoring, as proved by state or local law		

19

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					○ At the scene of a spill, or a suspected spill, of hazardous materials ○ For purposes of fire suppression ○ To rescue a person whose life or well-being is in imminent danger ○ By a Texas-licensed real estate broker in connection with marketing, sale, or financing of real property as long as no individual is identifiable in the image ○ Of real property or a person on real property that is within 25 miles of the U.S. border ○ From a height no more than 8 feet above ground level in a public place, AS LONG AS the image was captured without using any electronic, mechanical, or other means to amplify the image beyond normal human perception ○ Of public real property or a person on that property ○ 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 the state ○ In connection with oil pipeline safety and rig protection ○ In connection with port authority surveillance and security • DEFINITIONS: ○ Image = any capturing of sound waves,		

20

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					thermal, infrared, ultraviolet, visible light, or other electromagnetic waves, odor, or other conditions existing on or about real property in the state or an individual located on that property • Creates 2 criminal offenses related to the use of unmanned aircraft • Creates a civil cause of action for an owner or tenant of privately owned real property located in the state against a person who, in violation of the law, captured an image of the property or the owner or tenant while on the property. The statute of limitations for such a cause of action is 2 years from the date the image was captured or initially disclosed, displayed, distributed, or otherwise used.		
	HCR 217	Police ONLY	N/A	N/A	• Corrects the reporting requirements from HB 912	N/A	No regulation of retention, disclosure, or admissibility
Utah	SB 167 (Government Use of Unmanned Aerial Vehicles Act) Statutory Cite: UT ST § 63G-18-101 *et seq,*	Police AND Private Persons	YES	YES	• Generally prohibits police from obtaining, receiving, or using data acquired through a UAV • EXCEPTIONS: o Warrant o In accordance with judicially recognized exceptions to warrant requirements o From a person who is a nongovernment actor (as defined below) • DEFINITIONS: o UAV = an aircraft that is capable of sustaining flight and operates with no possible direct human intervention from	NO	• DISCLOSURE: A nongovernment actor may only disclose data acquired through a UAV to police if the data appears to pertain to the commission of a crime or the nongovernment actor believes, in good faith, that the data pertains to an imminent or ongoing emergency involving danger of death or serious bodily injury to an individual and disclosing the data would assist in remedying the emergency. • RETENTION: Police may not use, copy,

21

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
					on or within the aircraft and DOES NOT include an unmanned aircraft that is flown within visual line of sight of the individual operating the aircraft and strictly for hobby or recreational purposes ○ Nongovernment actor = a person that is not an agency, department, division, or other entity within state government; a person employed by or acting in an official capacity on behalf of the state; a political subdivision of the state; or a person employed by or acting in an official capacity on behalf of a political subdivision of the state ○ Target = a person upon whom, or a structure or area upon which, a person has intentionally collected or attempted to collect information through the operation of a UAV or plans to collect or attempt to collect information through the operation of a UAV		or disclose data collected by a UAV on a person, structure, or area that is not a target AND shall ensure that such data is destroyed as soon as reasonably possible after police collects or receives the data. BUT police is not required to comply if (a) deleting the data would also require deletion of data that relates to the target of the operation and is requisite for the success of the operation, (b) police receive the data through a court order that requires a person to release the data to the police or prohibits destruction of the data, or from a person who is a nongovernment actor, (c) the data was collected inadvertently and it appears to pertain to the commission of a crime, (d) police reasonably determine that the data pertains to an emergency situation and using or disclosing the data would assist in remedying the emergency, or (e) the data was collected through the operation of a UAV over public lands outside of municipal boundaries. • REPORTING: Creates reporting requirements for police No regulation of admissibility

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Vermont	No Currently Enacted Legislation, but Legislation Proposed or Pending						
Virginia	HB 2012 and SB 1331	Police ONLY	N/A	N/A	• Places a moratorium on the use of UAS until July 1, 2015 • EXCEPTIONS: ○ Amber Alert pursuant to VA Code § 52.34.3 ○ Senior Alert pursuant to VA Code § 52.34.6 ○ Blue Alert pursuant to VA Code § 52.34.9 ○ For search and rescue operations ○ Use by Virginia National Guard in certain circumstances	N/A	N/A
	Other Legislation is Proposed or Pending						
Washington	No Currently Enacted Legislation, but Legislation Proposed or Pending						
West Virginia	No Currently Enacted Legislation, but Legislation Proposed or Pending						

23

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Wisconsin	AB 203 and SB 196 Statutory Cite: WI ST 175.55, Use of drones restricted	Police AND Private Persons	YES	YES	• Generally prohibits police from using a drone to gather evidence or other information in a criminal investigation without first obtaining a search warrant • EXCEPTIONS: ○ Warrant ○ In an active search and rescue operation ○ To locate an escaped prisoner ○ Reasonable suspicion that use of a drone is necessary to prevent imminent danger to an individual or to prevent imminent destruction of evidence • DEFINITIONS: ○ Drone = a powered, aerial vehicle that carries or is equipped with a recording device (as defined in § 943.49(1)(c), that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, and can fly autonomously or be piloted remotely; can be expendable or recoverable • Makes it a Class H felony to sell, transport, manufacture, possess, or operate a weaponized drone • Makes it a Class A misdemeanor to use a drone to photograph, record, or otherwise observe another individual in a place where such individual has a reasonable expectation of privacy EXCEPT for police authorized to use a drone pursuant to the law	NO	• ADMISSIBILITY: Evidence or information collected in violation of the law is not admissible in evidence in any criminal proceeding No regulation of retention or disclosure

UAS Legal Memoranda, continued

STATE OR TERRITORY (Municipality, if applicable)	LEGISLATION, ENACTED OR PENDING	LEGISLATION APPLICABILITY (Police and/or Private Persons)	WARRANT REQUIRED (YES/NO)	EMERGENCY WARRANT EXCEPTION (YES/NO)	KEY LEGISLATIVE PROVISIONS	CIVIL CAUSE OF ACTION FOR VIOLATION (YES/NO)	REGULATION OF COLLECTED DATA
Wyoming	No Currently Enacted Legislation, but Legislation Proposed or Pending						

SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Building Public Understanding, Acceptance, and Confidence in Responsible and Constitutional Use of UAS Technology by Law Enforcement

TO: **The Police Foundation and the U.S. Department of Justice – COPS Office**

FROM: **Anne T. McKenna, Esquire**
Silverman|Thompson|Slutkin|White|LLC

RE: ***Community Policing and UAS Guidelines to Enhance Community Trust***
2013-CK-WX-K002
Building Public Understanding, Acceptance, and Confidence in Responsible and Constitutional Use of UAS Technology by Law Enforcement

DATE: **September 9, 2014**

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between the Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled, *Community Policing and UAS Guidelines to Enhance Community Trust* (the "COPS contract"). Pursuant to the COPS contract Task 8, this legal memorandum makes recommendations to build the public's understanding, acceptance, and confidence in responsible and constitutional use of Unmanned Aircraft System (UAS) and Unmanned Aircraft Vehicle (UAV) technologies.

UAS Legal Memoranda, continued

I. SUBJECT INTRODUCTION

Previous legal memos discussed the constitutional considerations and existing legal framework regulating law enforcement use of UAS technology;[1] UAV-collected data practices;[2] and liability and risk management concerns.[3] This legal analysis provides a proposed framework for domestic law enforcement's practices and policies with respect to use of UAV/UAS, and it identifies certain UAV/UAS usage that is improper and may violate constitutional doctrine and federal and state law.

Any police department seeking to build public understanding, acceptance, and confidence in its use of UAS technology should adhere to a consistent and uniform legal framework for acceptable UAS usage. Moreover, departments must implement policies and procedures designed to avoid any legal violations or perceived threat to its citizens' safety, privacy, and civil rights. This Memo discusses how police departments can build public understanding, acceptance, and confidence by educating the public on UAS technology and the various benefits it offers, and by maintaining community engagement, transparency, and accountability throughout the process of developing and employing these programs.

II. BUILDING PUBLIC UNDERSTANDING AND ACCEPTANCE: EDUCATING THE PUBLIC ON UAS TECHNOLOGY

Public skepticism over domestic use of UAS technology stems largely from misperceptions about the type of technology police departments will use, how the technology will be used by police, and why police departments seek to use it. Educating the public on UAS technology and the various benefits it offers is essential to building public understanding and acceptance of this technology. Law enforcement agencies seeking to implement UAS programs must clearly and consistently explain, educate, and demonstrate to the public:

(1) *What* UAS technology is, and what it is not;
(2) *How* this technology will and will not be used; and
(3) *Why* this technology is being used.

Media coverage of UAS technology focuses largely on weaponized drone strikes in warzones, leading the public to associate this technology with military force and violence. Public concern over police militarization has increased, particularly in light of events following the death of Michael Brown in Ferguson, Missouri. Thus, it is essential that law enforcement clearly identify the type of UAS technology and its use, while also explicitly differentiating military drones and dispelling these misconceptions.

In addition to fear of police militarization and physical violence, law enforcement must also address concerns over privacy risks posed by the use of UAS technology. These concerns are raised by uncertainty over the technological capabilities and degree of intrusiveness posed by the technology, as well as uncertainty over when and where UAS technology will be deployed.

[1] *See* Legal Memo: Police Use of UAVs and the Law.
[2] *See* Legal Analysis of UAV-Collected Data Practices.
[3] *See* Liability Analysis Memo.

Insecurity over how and why such technology will be used is another source of public skepticism toward domestic law enforcement use of UAS technology. The potential for constant police surveillance and resulting erosion of personal privacy threatened by unregulated UAS technology is frequently invoked by critics of UAS programs.

Fortunately, public concerns over police militarization, intrusive police surveillance, and indiscriminate privacy violations can be alleviated by educating the public on what UAS technology is being utilized, and how and why it is being used. The following practices designed to educate the public on UAS technology and dispel common misconceptions will help to build public understanding and acceptance of UAS technology.

A. *What* UAS Technology Is, and What it Is Not

- Provide a clear and simple explanation of the UAS technology, which should describe:
  - The UAS/UAV dimensions, technological capabilities, and other appropriate physical details;
  - Any additional technology with which the UAS may be equipped, such as video or audio recording equipment, facial recognition technology, thermal imaging cameras, etc.; and
  - Whether information gathered by UAS technology can be recorded or merely viewed in real-time.

- Illustrate how UAS technological capabilities are not materially different from existing police technology, such as stationary video camera surveillance, Automated License Plate Readers, helicopter surveillance, etc.

- Emphasize that UAS will never be equipped with any form of firearm or other weaponry.

- Clarify that domestic law enforcement UAS are not military drones and explicitly detail differences between these technologies.

B. *How* UAS Technology Will and Will Not Be Used

- Explain how the police department will ensure that use of UAS technology complies with constitutional requirements and federal law.

- Confirm that police department procedures will comply with any applicable state law regarding UAS technology.

- Specify how UAS technology will *not* be used, in light of constitutional and legal limitations, privacy and safety concerns, etc.

UAS Legal Memoranda, continued

- Provide a clear and precise outline of the scenarios in which use of UAS technology will be authorized. For example, UAS deployment may be authorized to:
  - Locate missing persons,
  - Respond to terrorist threats,
  - Assist first responders dealing with emergency situations,
  - Assess natural disasters, or
  - Monitor weather and wildlife.

- Identify whether UAS technology will be used in criminal investigations, as well as the search warrant requirements that must be satisfied for such use.

C. *Why* UAS Technology is Used by Law Enforcement

- Identify police department goals for the use of UAS technology.

- Explain the benefits of using this technology, such as reducing police department costs, ensuring officer and public safety, facilitating faster and more effective emergency responses, etc.

III. BUILDING PUBLIC CONFIDENCE: COMMUNITY ENGAGEMENT, TRANSPARENCY, AND ACCOUNTABILITY

Once the public understands and accepts UAS technology, police departments must build public confidence in UAS technology through community engagement, transparency, and accountability. Police must demonstrate to the public that the technology they are using and the manner in which they are using it are consistent with the public's expectations and sensitive to the public's privacy concerns. When use of UAS technology fails to meet these expectations, police departments must hold themselves accountable or risk losing the public's trust.

In order to collaborate with the community and proactively identify and address privacy concerns related to law enforcement use of UAS technology, police departments may wish to conduct a Privacy Impact Assessment (PIA). Modeled after the PIA required by the E-Government Act of 2002,[4] such an assessment would analyze what information is collected by UAS technology; when, how, and why this information is collected; disclosure and security of collected information; and "should address the impact the system will have on an individual's privacy."[5] Performing a PIA and disclosing the results prior to implementing UAS programs would demonstrate law enforcement's commitment to protecting the public's privacy and engaging the community to address its concerns.

Maintaining transparency with respect to UAS policy and procedures is also essential to building public confidence. Public skepticism of UAS technology stems from the misconception

[4] Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803.
[5] Memorandum from Joshua B. Bolten, Director, Office of Mgmt. and Budget to Heads of Executive Departments and Agencies, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), available at http://www.whitehouse.gov/omb/memoranda/m03-22.html.

that it will be used for widespread government monitoring of its citizens. To dispel this common myth, police departments should implement a standardized policy related to the collection, retention, and use of UAS-gathered data that is fully disclosed to the public. Inviting public comment on the department's data policy and providing public reports on data collection will also further public confidence.

The following practices designed to foster community engagement, transparency, and accountability will help to build public confidence in law enforcement's responsible and constitutional use of UAS technology:

- Conduct a Privacy Impact Assessment (PIA) to analyze the collection, storage, and use of information by the UAS technology and to address the program's impact on individual privacy.

- Invite public comment on proposed policies and procedures for UAS technology.

- Develop a specific data policy that includes procedures on data collection, retention, use, and disclosure.
    - Collection of electronic data by UAS/UAV must be conducted:
        - From a lawful vantage point
        - With a reasonably limited scope
        - In a non-discriminatory manner
    - Any data collection policy should address the following considerations:
        - Where data collection takes place;
        - What kind of data is collected;
        - How much data is collected; and
        - From whom the data is collected.
    - Where the data collected includes audio-recordings of protected communications, officers must comply with Title III of the Wiretap Act regarding authorization, minimization, and providing notice of the surveillance.
    - Data retention policies should specify:
        - Retention period: Length of data retention
        - Data storage: how data is stored, secured, and protected
        - Access: who may access the retained data and under what purposes
        - Use: for what purposes may the data lawfully be used
        - Disclosure: to what other persons or agencies may the data be disclosed
    - Data should be used and disclosed exclusively for law enforcement purposes, unless exigent circumstances warrant otherwise.

- Create publically-available, published guidelines that specify what happens to information once it is collected by UAS/UAV as well as how the collected information may or will be used. Such guidelines should discuss:
    - Whether captured data is retained or discarded;

UAS Legal Memoranda, continued

- If data is retained, officials should specify for how long data is retained and where it is retained, i.e., is a separate database maintained; is the data incorporated into other government databases?;
- What other government-controlled electronic databases the law enforcement agency compares captured data with (sex offenders, suspects wanted by police, etc.); and
- What actions the law enforcement agency takes when it detects a match.[6]

- Provide regular reports to the public on UAS missions and results, including data collection.

- Maintain accountability by requiring periodic outside review of the scope and effectiveness of the UAS technology program.

IV. CONCLUSION

Public concern over potentially limitless surveillance capabilities of sophisticated UAS/UAV technology stems largely from fear that officers will be watching and recording their every move. Law enforcement must combat this fear of covert surveillance and government secrecy with information and transparency regarding the technology, its use, and its benefits. As noted by the International Association of Chiefs of Police (IACP) in the 2014 "IACP Technology Policy Framework", a "principal tenet of policing is the trust citizens grant police."[7] Law enforcement must take reasonable steps to dispel concerns and foster public understanding, acceptance, and confidence in UAS technology in order to maximize the potential utility and public benefit offered by these emerging technologies.

[6] Max Guirguis, Electronic Visual Surveillance and the Reasonable Expectation of Privacy, 9 J. Tech. L. & Pol'y 143, 171 (2004).
[7] *See* International Association of Chiefs of Police Aviation Committee, *Recommended Guidelines for the use of Unmanned Aircraft* (Aug. 2012), *available at* http://www.theiacp.org/portals/0/pdfs/iacp_uaguidelines.pdf.

SILVERMCKENNA
The Internet and Privacy Law Group of STSW

LEGAL MEMORANDUM

TO: The Police Foundation and the U.S. Department of Justice – COPS Office

FROM: Anne T. McKenna, Esquire
Silverman|Thompson|Slutkin|White|LLC

DATE: June 23, 2014

RE: ***Community Policing and UAS Guidelines to Enhance Community Trust***

2013-CK-WX-K002

Legal Memorandum Number Five: UAS/UAV Related Publications, Law Review Articles, Research, and Peer Review Sources (Task 1 – Line Item (5))

LEGAL MEMORANDUM 5: OVERVIEW

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between The Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled "*Community Policing and UAS Guidelines to Enhance Community Trust*" (the "COPS Contract"). Pursuant to the COPS Contract Task 1 (detailed description of work appended to the COPS Contract), this memorandum ("Legal Memo 5") provides an overview and analysis of current research, law review articles, and other peer-reviewed publications on the benefits and problems associated with UAS usage.

Legal Memo 5 is structured as follows:

I. Overview of Recent Major Research Publications

II. Overview of Law Review Articles (in reverse chronological order)

III. Overview of In-depth Media Articles from the Prior Calendar Year (in reverse chronological order)

IV. Citation to Blogs with UAS/UAV-related Posts that Have High Web Traffic

V. Overview of Peer Review Publications and Peer Published Guidance

---

UAS Legal Memoranda, continued

I. OVERVIEW OF RECENT MAJOR RESEARCH PUBLICATIONS

A. ***2013 Unmanned Aircraft Systems (UAS) Legislation***, NATIONAL CONFERENCE OF STATE LEGISLATURES, *available at:* http://www.ncsl.org/research/civil-and-criminal-justice/unmanned-aerial-vehicles.aspx.

This article lists and describes every law enacted in state legislatures in 2013 surrounding UAS usage and regulations. Over the course of the year, 43 states introduced 130 bills and resolutions, resulting in 16 new laws and resolutions enacted by 13 different states. Laws include definitions of drones, regulation of who may use UASs and for what circumstances, what types of data may be collected, as well as funding for drone research. For a full description of each statute, visit the above link.

B. ***Integration of Civil Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS) Roadmap***, FEDERAL AVIATION ADMINISTRATION, U.S. DEPT. OF TRANSPORTATION, Nov. 7, 2013. *available at:* http://www.faa.gov/about/initiatives/uas/media/uas_roadmap_2013.pdf

This roadmap outlines the steps the FAA needs to take in order to safely integrate UASs into the National Airspace System, in accordance with the Congressional Mandates in the *FAA Modernization and Reform Act of 2012*. It includes goals, metrics, and target dates for the use of the FAA and its government and industry partners in implementing key actions for UAS integration. It includes a description of proposed civil and commercial applications of drone usage, as well as an outline of current FAA UAS policies and the basis for them. The roadmap then enters a discussion of privacy and civil liberties considerations in regards to UAS usage and the operational tests sites to be utilized by the FAA, and states that each test site will implement a privacy policy guided by the Fair Information Practice Principles. The discussion of privacy and civil liberties is brief, and the focus of the publication is safe operation and usage as well as federal safety regulations and licensing procedures.

C. ***Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses***, Richard M. Thompson II, CONGRESSIONAL RESEARCH SERVICE, Apr. 3, 2013.

The author begins by defining drones and identifies current and future technologies that could be outfitted to drones. The author then undergoes a thorough examination of the Fourth Amendment jurisprudence, including what constitutes a search in the home, open fields, in public airspace, along U.S. borders as well as prolonged searches. This is the most thorough of these resources. The author also includes the best arguments for and against the use of drones in certain scenarios based on past Supreme Court precedent. Considerations for whether use of drone surveillance is a search include location, sophistication of technology used, and duration of surveillance. Whether a targeted individual is at home, in his backyard, in the public square or near a national border will play a large role in determining whether he/she is entitled to privacy. Aerial surveillance cases (*Ciraolo, Riley, Dow*) were premised on naked eye searches. The sophistication of the technology available (facial recognition, thermal imaging, etc.) to drones may diminish the relevance of this prior jurisprudence. Drones have the ability to break down any practical privacy safeguard. Drones can see things from several angles, which raises the

question: should people have to account for that when demonstrating subjective expectation of privacy? In consideration of duration of surveillance, some case law already exists. In the Fifth Circuit case, *US v. Cuevas-Sanches*, law enforcement put a video camera on a utility pole overlooking the defendant's 10-foot-high fence surrounding his backyard. The 5th Circuit said the video camera was a search. On the subject of drones and warrants, the author argues that if law enforcement is using drones for a need other than law enforcement (Special Needs Doctrine, uses such as search and rescue missions, environmental protection, etc.), drones will probably be found constitutional. However, if drones are used primarily for law enforcement purposes, a warrant may be required unless one of the exceptions applies.

D. ***Privacy Impact Assessment for the Robotic Aircraft for Public Safety (RAPS) Project***, John Appleby, U.S. DEPARTMENT OF HOMELAND SECURITY, Nov. 16, 2012.

The DHS applies Fair Information Practice Principles (FIPP) to DHS programs and activities that raise privacy concerns or involve collection of personally identifiable information from individuals. The DHS applied their FIPP (developed from the underlying concepts of the Privacy Act of 1974) to test the use of drones by the first responder community. The test used drones equipped with sensors and cameras that could captures images and transmit them to a ground control system, but did not include technology such as facial recognition. However, DHS conducted this evaluation on a test group, meaning that everyone participating the study volunteered and many of the privacy concerns by the everyday public do not apply. The DHS considers the following principles: Transparency, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

II. OVERVIEW OF RECENT LAW REVIEW ARTICLES

A. *Anonymity, Faceprints, and the Constitution*, Kimberly N. Brown, 21 GEO. MASON L. REV. 409 (Winter 2014).

Brown's article argues for recognition of anonymity as a constitutional value that is both implicit in Fourth Amendment jurisprudence and explicit in First Amendment jurisprudence, and suggests that a modern shift in technology's intersection with data warrants a fresh look at Fourth Amendment doctrine that currently excuses surveillance based on information obtained in public or from third parties. Brown commences by defining "anonymity" and exploring the historical background of the concept, arguing that "respect for the capacity to remain physically and psychologically unknown to the government traces back" to the founding of our nation. Brown also discusses facial recognition technology (FRT) and various concerns and harms related thereto. Brown then reviews the existing Fourth and First Amendment jurisprudence (dividing the Fourth Amendment discussion into two sections: the pre-digital age and the digital age) that, arguably, identifies anonymity as a constitutional value warranting more explicit doctrinal protection. Finally, Brown argues that our constitutional jurisprudence should be reconciled to address the manipulation – as opposed to acquisition – of FRT data to derive new and exceedingly intimate information about individuals. Brown also offers guidelines for consideration by lower courts and legislators as they address the threat of limitless surveillance presented by new technologies such as FRT

UAS Legal Memoranda, continued

B. *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Ben Jenkins, 102 KY. L.J. 161 (2013–2014).

Jenkins, a 2014 graduate, argues that in order to safeguard privacy against UAS surveillance by the government, Congress should implement legislation that provides a framework for protection while still allowing for industry growth and innovation. Jenkins starts with a discussion of the background of drones and their legal landscape, specifically what they are, their various uses, the available technology, and the current Fourth Amendment jurisprudence. Jenkins then explains why, in his view, drones present a unique threat to privacy, addressing current shortfalls in Fourth Amendment jurisprudence and in legislative efforts to address the public's privacy concerns. Jenkins suggests amending the proposed legislation to address shortfalls therein, concluding that proper anticipatory action and ongoing oversight are necessary to ensure that police technology does not erode the minimum expectations of privacy guaranteed by the Fourth Amendment.

C. *Contextual Expectations of Privacy,* Andrew D. Selbst, 35 CARDOZO L. REV. 643 (Dec. 2013).

Selbst evaluates the modern meaning of the Fourth Amendment's "reasonable expectation of privacy" in the light of Helen Nissenbaum's theory of contextual integrity. The theory of contextual integrity states that privacy is essentially the right to an appropriate flow of personal information. What flow of information is deemed as "appropriate" is based on social expectations and social contexts, and therefore the structure of the "informational norm" varies widely. Selbst includes a description of the current method generally used by the courts to determine if there has been a Fourth Amendment violation—the *Katz* test—and points out some flaws with this method. For example, if information is accessible to anyone other than a government official—such as bank records and lists of phone numbers a person frequently calls—then it is outside the scope of the Fourth Amendment. The logic of *Katz*, Selbst argues, is circular: if a person knows he or she is being watched, he or she must expect to be watched, therefore limiting circumstances in which a person has a justifiable expectation of privacy. If this theory is pressed, it presents the possibility of the complete erosion of privacy. Selbst then goes on to address multiple situations in which privacy is concerned, and how the theory of contextual integrity can be implemented to define reasonable and unreasonable expectations of privacy.

D. *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat Through Interagency Coordination*, Patrice Hendriksen, Note, 82 GEO. WASH. L. REV. 207 (Dec. 2013).

Hendriksen, a 2014 graduate, argues that Congress should amend the FAA Modernization and Reform Act of 2012 (FMRA) to mandate interagency coordination with the ultimate goal of creating a Memorandum of Understanding that clarifies responsibilities, recommends permissible use guidelines, and creates accountability for the privacy implications related to the integration of UAS into law enforcement functions. Hendriksen concludes that such an amendment would effectively address the complexity of UAS operations and close the currently existing privacy gap in the law. Hendriksen commences the Note with the factual and legal background for his/her analysis, setting forth the current and projected status of domestic UAS use with a discussion of the FMRA and UAS technology. Hendriksen then addresses the

relevant Fourth Amendment jurisprudence and analyzes surveillance *via* UAS under the Fourth Amendment. In this regard, Hendriksen concludes that applying the Fourth Amendment to UAS surveillance yields uncertain and insufficient limitations. Thus, Hendriksen proposes that Congress amend the FMRA to compel interagency coordination regarding the privacy threat posed by UAS technology. Finally, Hendriksen identifies and discusses legislative and single-agency counterproposals, highlighting their inadequacies.

E. *THE DRONES ARE COMING! Will the Fourth Amendment Stop Their Threat to Our Privacy?* Robert Molko, 78 BROOK. L. REV. 1279 (Summer 2013).

Molko analyzes the protection the Fourth Amendment offers in the face of the increasingly common usage of drones by local law enforcement to monitor criminal activity in communities. Molko begins the article with a brief summation of current drone technology and usage, and the FAA Modernization and Reform Act of 2012. He then discusses the difficulty of using the Katz test to aid courts to determine a citizen's privacy expectations when it comes to drones. Despite these difficulties, however, Molko argues that this test can be applied in new ways to effectively protect privacy while still enabling the government to adequately provide security for its citizens. One of the main privacy concerns surrounding long-term drone surveillance is that the accumulation of information would give government unprecedented ability to sort through this information to find a collection of minute details which, in conjugation, could allow a person to be convicted of a crime. Molko suggests this power be limited via a congressionally mandated limit on drone data storage in situations where there is no reasonable suspicion that criminal activity is occurring in the surveilled area. Until Congress acts, however, Molko states that the courts can use the reasonable expectation of privacy test to outline the boundaries of drone usages by the government.

F. *Over Your Head, Under the Radar: An Examination of Changing Legislation, Aging Case Law, and Possible Solutions to the Domestic Police Drone Puzzle*, J. Tyler Black, Note, 70 WASH. & LEE L. REV. 1829 (Summer 2013).

Black, a 2014 graduate, argues that though drones' potential for a positive impact on society is substantial, they also carry the potential for abuse because the technology can outstrip certain constitutional protections and case law governing naked-eye aerial observation by police. Black commences by surveying drone capabilities and providing background on FAA drone regulations prior to the FAA Modernization and Reform Act of 2012 (FMRA). Black then briefly explores the FMRA, which expanded the use of drones domestically. Black provides an overview of the Supreme Court's aerial observation case law, discussing the "widening divergence in the application" of this jurisprudence. Black concludes the Note by listing possible legislative and judicial remedies and suggestions that arguably would guard against inappropriate drone use by police.

G. ***Floating Toward a Sky Near You: Unmanned Aircraft Systems and the Implications of the FAA Modernization and Reform Act of 2012*, Brandon Bellows, 78 J. AIR L. & COM. 585 (Summer 2013).**

Bellows, a 2014 graduate, commences his Comment with a hypothetical designed to bring light to the privacy, safety, and compliance issues surrounding the use of UASs. Bellows

UAS Legal Memoranda, continued

then traces the evolution of the UAS from a military tool to a non-military domestic instrument and surveys current and future UAS use. Bellows reviews the current state of UAS law, focusing particularly on the FMRA and its provisions for UASs in the national airspace, and briefly highlighting state-level rumblings about UAS regulation and states' efforts to remedy apparent deficiencies spotted in the FAA's forthcoming UAS regulatory scheme. Finally, Bellows analyzes the developing FAA regulatory scheme for UASs, making broad suggestions about certain topics such as safety and privacy.

H. ***The Drones Are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and Its Fourth Amendment Implications*, Philip J. Hiltner, 3 WAKE FOREST J.L. & POL'Y 397 (June 2013).**

Hiltner, a 2013 graduate, explores how the opportunity for technology enhanced aerial surveillance via UASs implicates Fourth Amendment issues. Hiltner commences by providing background on the current capabilities of UASs. Hiltner then briefly explains the current FAA regulations regarding UASs and the FAA Modernization and Reform Act of 2012. Hiltner discusses how Fourth Amendment jurisprudence regarding surveillance of the home might affect police usage of drones and also looks at police drone usage for general public surveillance. Finally, Hiltnre concludes by offering suggestions of steps that could be taken to allow police forces to capitalize on the many advantages UASs provide without diminishing the public's privacy expectations.

I. ***Warrantless Government Drone Surveillance: A Challenge to the Fourth Amendment*, Jennifer O'Brien, 30 J. INFO. TECH. & PRIVACY L. 155 (Spring/Summer 2013).**

O'Brien, a 2014 graduate of The John Marshall Law School, posits that "the drone presents one of the greatest challenges to society's privacy expectations under the Fourth Amendment." O'Brien commences her Comment by providing an overview of drone capabilities and the current FAA regulation on drones. O'Brien then details Fourth Amendment jurisprudence with regards to various forms of surveillance employed by the government and discusses the anticipated application of that case law to government use of drones within the U.S. O'Brien concludes with a discussion of the changes that need to be made in the Supreme Court's Fourth Amendment analysis in order to adequately protect the public's privacy interests without unduly burdening law enforcement.

J. ***Observations From Above: Unmanned Aircraft Systems and Privacy*, John Villasenor, 36 HARV. J.L. & PUB. POL'Y 457 (Spring 2013).**

Villasenor considers the constitutional, statutory, and common law frameworks that will inform privacy rights with respect to observation *via* unmanned aircraft. Villasenor begins the article with a discussion of the history of UAS technology and a description of the technology available today. He then addresses the current regulatory environment in the U.S., paying particular attention to the FAA Modernization and Reform Act of 2012. Villasenor examines the application of the Supreme Court's Fourth Amendment jurisprudence to government operation of unmanned aircraft, discussing in detail certain cases (*Dow*, *Ciraolo*, *Riley*, *Kyllo*, *Jones*) as well as the interpretations they suggest regarding the constitutionality of surveillance *via* UAS. Villasenor also addresses the operation of UAS by private entities and explores the laws that

might be used to combat violations of privacy by private entities and individuals. Villasenor concludes the article by considering potential new voluntary and statutory privacy solutions and discussing the preemption issues that may arise when non-federal entities attempt to regulate UAS use. Villasenor ultimately concludes that the Constitution will provide a much stronger measure of protection against government UAS privacy abuses than is generally appreciated.

K. ***The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights*, Chris Schlag, 13 U. PITT. J. TECH. L. & POL'Y 1 (Spring 2013).**

Schlag, a 2014 graduate, suggests that the best way to ensure that our individual privacy rights are not eroded by the incorporation of drone technology into our daily lives is for Congress to enact a baseline consumer protection law that manages both governmental and private party use of drones in national airspace. Schlag begins by discussing the history and development of drone technology and the domestic integration of drones. Schlag then evaluates various Fourth Amendment privacy issues arising out of domestic drone use, specifically within the context of surveillance and technology development, and examines current regulatory schemes, administrative controls, and available judicial protections. The article then considers potential solutions to those privacy concerns and argues that the FAA and state legislative enactments alone fail to guard against privacy invasions from both publicly and privately operated domestic drones. Schlag concludes by summarizing the necessity of a baseline federal consumer protection law which would, arguably, ensure drone-use practices by police or private parties do not violate reasonable expectations of privacy.

L. ***The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones*, Matthew L. Burow, 39 New Eng. J. on Crim. & Civ. Confinement 427 (Spring 2013).**

Burow, a 2013 graduate, commences this Note by reviewing the Supreme Court's Fourth Amendment and aerial surveillance jurisprudence, arguing that those decisions do not protect modern society from the intrusiveness of UASs. Burow also argues that *U.S. v. Jones*, addressing law enforcement's use of GPS technology, may pave the way for the protection of public anonymity. Burow then explores the concept of anonymity in public spaces and discusses the psychological and societal ramifications of a "Big Brother" surveillance society. Burow further explores areas where the legislature can take immediate action to help prevent constant UAS surveillance, arguing that both federal and state legislatures need to do their part to legitimize the constitutionally enumerated right to anonymity.

M. ***Drones and Privacy*, Timothy T. Takahashi, 14 COLUM. SCI. & TECH. L. REV. 72 (Mar. 23, 2013).**

Dr. Takahashi introduces the subject of government surveillance *via* UAS by relating the story of the June 23, 2011, Predator drone-assisted arrest of the owner and inhabitants of a North Dakota ranch. Takahashi first examines whether Posse Comitatus and/or the Fourth Amendment were violated during this particular arrest, concluding that a defense argument on either of those grounds was, in that case, unlikely to be successful. Takahashi then details the various technologies that UAV/UASs can be outfitted with. Takahashi makes an interesting point

UAS Legal Memoranda, continued

relevant to data retention issues: "Traditional police eavesdropping and surveillance required humans to personally investigate and observe other humans in action. Advances in digital storage technology enable permanent storage of extraordinarily detailed data. Law enforcement need no longer prospectively observe behavior to take action; they may retrospectively review archived surveillance data." 14 COLUM. SCI. & TECH. L. REV. 72, 92.

Takahashi then delves into the history of Fourth Amendment jurisprudence, addressing the traditional property law roots of the Fourth Amendment and detailing the evolution of Fourth Amendment protections. He further examines modern-day Fourth Amendment jurisprudence as it relates to new technologies, concluding that "the *Katz* "reasonable expectation of privacy" standard has already reached its breaking point when applied to emergent surveillance technology." Ultimately, Takahaski concludes that because of the multitude of technologies that can be leveraged with UASs, it is likely that the Supreme Court will need to re-evaluate the current constitutional paradigm for privacy.

N. ***Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights*, Alexandra Rengel, 8 INTERCULTURAL HUM. RTS. L. REV. 177 (2013).**

This article, derived from the Intercultural Human Rights Law Review Annual Symposium held October 19, 2012, addresses more than just the "privacy threat" posed by UASs. In the short section addressing UASs directly, Rengel briefly defines and describes UASs, their capabilities and advantages, their regulation by the FAA, and the general privacy concerns surrounding their use. According to Rengel, "[p]rivacy concerns, regarding unmanned aerial vehicles, center on the fact that these vehicles provide almost limitless access to view and record events from the sky, without the consent or knowledge of those being surveyed." 8 INTERCULTURAL HUM. RTS. L. REV. 177, 203.

The takeaway from Rengel's article is that "[t]he law needs to be proactive regarding privacy issues. [. . .] In order to achieve better results, jurists and legislators must partner with designers and manufacturers of technology, as well as privacy and other experts, to create laws that address potential issues regarding privacy." 8 INTERCULTURAL HUM. RTS. L. REV. 177, 228.

O. ***Drones in the Homeland: A Potential Privacy Obstruction under the Fourth Amendment and the Common Law Trespass Doctrine,* Ajoke Oyegunle, 21 COMMLAW CONSPECTUS 365 (2013).**

Oyegunle, a 2014 graduate, begins by outlining some concerns of the FAA Modernization and Reform Act of 2012, including its failure to inform the American public of the impending large-scale integration of UASs into the National Airspace System, its failure to list requirements for applicants to attain approval to deploy drones, and its failure to articulate who may utilize drones and for what purposes. The Act also directs the FAA to simplify the process for government agencies to obtain licenses to drones, a concerning direction given the bounty of privacy concerns that drones create. Oyegunle then examines the constitutional and common law implications of domestic drone use, discussing aerial surveillance and trespass doctrine case law, surveillance technology, and applying equilibrium-adjustment theory and mosaic theory analyses. Finally, Oyegunle presents the potential benefits and harms of drones, as

well as possible solutions. Oyegunle ultimately concludes that before the FMRA is implemented, comprehensive privacy safeguards must be instituted.

P. ***Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Jonathan Olivito,74 OHIO ST. L.J. 669 (2013).**

Olivito, a 2014 graduate, is the first (and possibly only) legal scholar to argue that courts should analyze drone surveillance challenges under the assumed constitutional right to informational privacy as first articulated by the Supreme Court in *Whalen v. Roe*. Under this approach, the courts would apply a balancing test that weighs the individual privacy interests against the government interests in drone surveillance and, in the case of a violation, would then prohibit the government from storing, aggregating, transferring, or distributing any information gathered in the challenged surveillance. Olivito further notes that this proposed balancing test and remedies could apply broadly to other public surveillance systems that gather and aggregate extensive amounts of information (*e.g.*, license plate readers and city-wide cameras/CCTV). Olivito commences by examining the physical capabilities of drones and describing their current and potential future domestic applications. Olivito then explains why, in his view, current Fourth Amendment jurisprudence and statutory, regulatory, and tort law provide inadequate protections against drone privacy intrusions. Olivito analyzes the current application of the constitutional right to informational privacy and the right's disparate application among the circuits. Olivito then argues that courts should use the constitutional right to informational privacy when confronted with claims of privacy intrusion involving drone surveillance.

Q. ***Unmanned But Accelerating: Navigating the Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System*, Benjamin Kapnik, 77 J. AIR L. & COM. 439 (Summer 2012).** In this article, Kapnik, a 2013 graduate of George Washington University Law School, addresses the short-term regulatory and privacy hurdles facing the unmanned aircraft industry. Kapnick commences by discussing the difficulty of defining "unmanned aircraft" and examining the existing and then-forthcoming regulations and statutes governing unmanned aircraft. Kapnick then examines the impact of privacy law on the operation of UAVs by both government and private entities or individuals, discussing both Fourth Amendment jurisprudence (*Katz*, *Ciraolo*, *Riley*, *Kyllo*) (with a section devoted entirely to *Jones*) and criminal and civil privacy statutes and common law. Kapnik concludes that unmanned aircraft are on their way and the legal system must adjust accordingly.

R. ***Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations*, Paul McBride, 74 J. AIR L. & COM. 627 (Summer 2009).** McBride, a 2010 graduate of Southern Methodist University Dedman School of Law, commences by discussing the development and modern applications – both military and civilian/law enforcement – of UAS technology. McBride then considers the evolution of Supreme Court precedent regarding warrantless surveillance, aerial surveillance in particular. McBride then analyzes the use of UASs in domestic surveillance in light of existing Supreme Court jurisprudence, arguing that the surveillance of the curtilage of the home using UAS platforms and technologies is a search under the Fourth Amendment. McBride concludes this Comment by noting that future developments as to both the composition of the Supreme Court and the availability of certain technologies may significantly impact the resolution of the constitutionality of UAS surveillance.

UAS Legal Memoranda, continued

S. ***Big Brother Will Soon Be Watching—Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement*, Joseph J. Vacek, 85 N.D. L. REV. 673 (2009).**

In this article, which significantly pre-dated the FAA Modernization and Reform Act of 2012, Vacek concludes that the eventual use of UAVs in domestic law enforcement is a near certainty, which will require the Supreme Court to reevaluate our notions of privacy under the Fourth Amendment and reasonable searches under *Kyllo*. Vacek begins by addressing the background issues posed by government use of UASs, providing an overview of available UAVs/UASs, a discussion of the current U.S. regulatory scheme, and an examination of the constitutional limitations on aerial surveillance. Vacek then illustrates the burdensome process a local law enforcement agency had to endure (at the time of publication) to utilize UAVs in operations. Vacek's article then addresses various then-recent regulatory developments regarding the operation of small UAVs. The article concludes by exploring where Fourth Amendment jurisprudence might go when we're faced with continuous, ubiquitous airborne surveillance.

T. ***The Integration of Unmanned Aerial Vehicles Into the National Airspace*, Timothy M. Ravich, 85 N.D. L. REV. 597 (2009).**

In this article, which significantly pre-dated the FAA Modernization and Reform Act of 2012, Ravich argues that UAV operations have outpaced the law and that given the actual proliferation of UAVs, it is time for lawmakers to more directly address UAV integration into the national airspace as a matter of law. Ravich commences with a brief background of the way in which the law has historically dealt with air and land rights relative to new and unprecedented developments in aviation. Ravich then discusses the operative regulatory regime in existence (at the time of publication), evaluates its fitness in the UAV context, and introduces the development of UAV-related laws in foreign jurisdictions.

U. ***Unmanned Aerial Exposure: Civil Liability Concerns Arising from Domestic Law Enforcement Employment of Unmanned Aerial Systems*, Geoffrey Christopher Rapp, 85 N.D. L. REV. 623 (2009).**

As the title suggests, Rapp's article addresses civil liability concerns related to police use of UAVs/UASs, concluding that civil litigation will inevitably follow the coming UAV revolution. Rapp commences by examining what might go wrong and hypothesizing worst-case scenarios in various contexts (*e.g.*, ground damage, air-to-air collision, communications interference, constitutional rights and privacy, landowner's rights, environmental concerns, and piracy). Rapp then provides an overview of existing aviation liability law and details the special doctrines of governmental immunity that protect law enforcement authorities from civil litigation, specifically addressing any special considerations likely to arise from the introduction of UAVs into the national airspace and the integration of UAV-related civil claims into the existing body of aviation tort law. Rapp concludes by addressing selected additional legal considerations, specifically conflicts of laws and insurance law.

III. OVERVIEW OF IN-DEPTH MEDIA ARTICLES

A. **FORBES:**

Sean Lawson, *Next Moves in the Battle Over Domestic Drones*, FORBES, Apr. 22, 2014, *available at* http://www.forbes.com/sites/seanlawson/2014/04/22/next-moves-in-the-battle-over-domestic-drones/print/.

In this *Forbes* article, Sean Lawson reports on the FAA decision to launch an official investigation into the use of small drone over the 4/20 rally in Denver, Colorado. Lawson posits that the FAA's actions are arbitrary and capricious, and that people recognize and accept the various socially beneficial uses of drones. However, the main takeaway from this article is that "peoples' primary concern is government, in particular law enforcement, use of [drone] technology for surveillance."

Gregory McNeal, *DOJ Report Reveals Details of Domestic Drone Usage*, FORBES, Sept. 28, 2013, *available at* http://www.forbes.com/sites/gregorymcneal/2013/09/28/doj-report-reveals-details-of-domestic-drone-usage/print/.

In this *Forbes* article, Gregory McNeal reports that as of May 2013, four U.S. Department of Justice agencies were testing or using drones to support their operations. Specifically, the FBI has actually used drones to support its operations, ATF plans to deploy drones to support future operations, and the DEA and the U.S. Marshals Service have acquired drones but do not have plans to deploy them operationally. According to the DOJ Inspector General report, officials from the FBI and ATF have developed procedures regarding how they will operate drones but contended that they did not need to develop special drone privacy protocols, seeing no difference between drones and manned aircraft. The Inspector General, however, disagreed with this assessment and recommended that the Office of the Deputy Attorney General convene a working group to address this issue.

B. **U.S.A. TODAY:**

Sandy Johnson, *Balancing Privacy, Jobs in the Domestic Drone Debate*, U.S.A. TODAY, Apr. 11, 2014, *available at* http://www.usatoday.com/story/news/nation/2014/04/11/stateline-privacy-jobs-drones/7590409/.

In this article that appeared in multiple news sources, U.S.A. Today among them, Sandy Johnson reports on North Dakota's wholly unique approach to drones. North Dakota police do not need a warrant to use drones and the state has not enacted any drone laws. Instead, drone flights are overseen by Alan Frazier, an associate professor at University of North Dakota, who is in charge of the Law Enforcement Unmanned Aircraft Systems Research Project. Frazier reports to a university compliance panel that specified five situations in which drones may be used: to search for lost people; perform post-disaster assessments; photograph crime and accident scenes; search for crime suspects who pose a risk to public safety; and assist with traffic control at major events. Frazier's assessment is that no warrant is needed to fly drones: "It's not a drone concern – it's an information technology concern. The real concern is what's happening with that data."

C. **NEW YORK TIMES:**

Matthew L. Wald, *F.A.A. Picks Diverse Sites to Carry Out Drone Tests*, N.Y. TIMES, Dec. 30, 2013, *available at* http://www.nytimes.com/2013/12/31/us/politics/us-names-domestic-test-sites-for-drone-aircraft.html?_r=0&pagewanted=print.

UAS Legal Memoranda, continued

In this New York Times article from December 2013, Matthew Wald reports on the FAA selection of various institutions to operate UAV/UAS test sites throughout the United States. Though the article does not disclose the location(s) of the test sites, the institutions selected to do the testing include Griffiss International Airport (a former Air Force base near Rome, NY), Virginia Tech (who has an agreement to work with Rutgers University in NJ), the University of Alaska, the State of Nevada, the North Dakota Department of Commerce, and Texas A&M University Corpus Christi. The testing will explore how to set safety standards, how to train and certify ground-based pilots, how to ensure that the aircraft will operate safely even if radio links are lost, and how to replace the traditional method for avoiding collisions. The FAA has put several privacy requirements in place for the test program, for example, site operators will be required to publish privacy policies covering how the data gathered will used and how long it will be retained. Michael P. Huerta, the administrator of the FAA, envisions that integration of UAV/UAS into the national airspace will be a staged process.

Anne Eisenberg, *Preflight Turbulence for Commercial Drones*, N.Y. TIMES, Sept. 7, 2013, *available at* http://www.nytimes.com/2013/09/08/business/preflight-turbulence-for-commerical-drones.html?pagewanted=print.

In this *New York Times* article, Anne Eisenberg briefly addresses the perceived benefits or advantages and concerns surrounding commercial use of drones. Eisenberg notes that several states are legislatively limiting the use of drones and that local groups have arisen in opposition to the use of drones by the government. According to Jay Stanley, a senior policy analyst at the ACLU, it comes down to putting in place privacy protection "so that people can innovate around this technology without the cloud of Big Brother hanging over them."

Somini Sengupta, *U.S. Border Agency Allows Others to Use Its Drones*, N.Y. Times, July 3, 2013, *available at* http://www.nytimes.com/2013/07/04/business/us-border-agency-is-a-frequent-lender-of-its-drones.html?pagewanted=all&pagewanted=print.

In this *New York Times* article from last summer, Somini Sengupta reports on the lending of Customs and Border Protection-owned Predator drones to other domestic agencies, including for example, the FBI, the North Dakota Army National Guard, the Texas Department of Public Safety, and the U.S. Forest Service. Some of the commonly voiced concerns mentioned in the article relate to privacy and data practices and policies, the potential that CBP plans to weaponize its drones, and "indiscriminate" surveillance. For the record, CBP has stated that "when conducting joint operations with state, local and other federal agencies, its own privacy policies govern the use of data collected by the drones and 'the live feed from any aircraft is encrypted and only accessible to those with specific clearance.'"

D. **THE ECONOMIST:**

***Unmanned Aircraft: Game of Drones*, THE ECONOMIST, Dec. 21, 2013**, *available at* http://www.economist.com/node/21591862/print.

This article from the print edition of *The Economist* details, once again, the arguments we keep hearing from both drone proponents and detractors. Compare the following quote from Lucien Miller of Innov8tive Designs, a UAS firm in San Diego county: "The good stuff you can

do is endless," with the paragraph addressing detractors' concerns: "Polls find deep public concern over the privacy implications of drones. Some cities have banned them altogether, albeit probably temporarily. One Colorado town is considering allowing locals to shoot drones from the sky, and may offer rewards for recovering their parts."

E. **NEWSMAX:**

David Alan Coia, *US Domestic Drone Use Sidesteps Warrants for Thermal Imaging*, NEWSMAX, Aug. 11, 2013, *available at* http://www.newsmax.com/PrintTemplate.aspx/?nodeid=519767.

In this article from Newsmax, David Alan Coia reports on the FBI's use of surveillance drones equipped with thermal imaging devices as revealed in written communication between Stephen D. Kelley, assistant director of the FBI's office of Congressional Affairs, and Senator Rand Paul (R-Ky.). The FBI disclosed that it has used drones in eight criminal cases and two national security cases, and that in none of these instances did it acquire a search warrant or judicial order. The FBI's stated policy is that it "will not use UAVs to acquire information in which individuals have a reasonable expectation of privacy under the Fourth Amendment." But when Sen. Paul asked for clarification about the interpretation being applied regarding "reasonable expectation of privacy," he was referred to the FBI's partially classified Domestic Intelligence and Operations Manual. Interestingly, the spokesman for the FAA, Les Dorr, stated that "The FAA's sole mission is safety, so as far as what someone would put on an unmanned aircraft is relevant to us only to the extent that it would affect the airworthiness of the unmanned aircraft. We don't regulate the actual use of them."

F. **WASHINGTON LAWYER:**

Sarah Kellogg, *Drones: Coming to the Skies Near You*, WASHINGTON LAWYER, July–Aug. 2013, at 22, *available at* https://www.dcbar.org/bar-resources/publications/washington-lawyer/articles/july-august-2013-drones.cfm. T

his article from the July/August 2013 issue of the D.C. Bar's journal, provides an in-depth look at drones, addressing the following topics: the military history of drones; the thorny legal issues raised by using weaponized drones in the war on terror; the numerous commercial and law enforcement benefits offered by drones; the challenges faced in integrating drones into our national airspace; the legislative efforts to limit the use of drones domestically; the privacy concerns related to using drones for surveillance and data-gathering; and the potential future issues that may arise as drones become autonomous.

IV. CITATION TO BLOGS WITH UAS/UAV-RELATED POSTS THAT HAVE HIGH WEB TRAFFIC

- http://www.pbs.org/newshour/bb/science/jan-june13/drones_04-18.html
- http://www.npr.org/2012/04/17/150817060/drones-move-from-war-zones-to-the-home-front

UAS Legal Memoranda, continued

- http://www.theatlantic.com/politics/archive/2013/05/obamas-domestic-drone-standard-is-now-tighter-than-rand-pauls/276188/

V. OVERVIEW OF PEER REVIEW PUBLICATIONS AND PEER PUBLISHED GUIDANCE

A. ***Special Operations Standard Operating Procedures*, ARLINGTON, TX POLICE DEPT., Mar. 3, 2013.**

This SOP from the Arlington, Texas Police Department provides an incredibly comprehensive guide to operating a drone and the safety precautions to be considered before, during, and post flight. However, it provides scant guidelines for law enforcement about what use may be constitutional under the Fourth Amendment, especially in relation to advanced technologies which may be attached to the drone. Procedures are very safety conscious and comprehensive, and include the training of pilots and observers (an observer is required to maintain a line of sight of the drone and to assist the pilot in carrying out all safety requirements) and pre-flight briefings considering factors such as weather. A camera operator will also receive training on the camera and sensing equipment operations. Procedures include flight requirements used prior to a mission. This section also notes interesting considerations for pilots and their supervisors prior to flight. While they are listed for safety reasons, there is some Fourth Amendment overlap in these conditions. Safety procedures avoid "air-to-air" conflict including communication with air traffic control. The Procedures list prohibits acts including using a drone when a warrant is required, but these are not specific. While the Arlington, Texas procedures are one of the more comprehensive procedural guidelines on drones, they do not provide working legal guidelines for officers in the field.

B. ***Recommended Guidelines for the use of Unmanned Aircraft,* INT'L ASS'N OF CHIEFS OF POLICE, AVIATION COMMITTEE, Aug. 2012.**

The IACP is helpful for its broad policy recommendations. For example, it discourages the use of weapons and other enhanced technology while utilizing drones and gives guidance on when a search warrant is required. However, it is not very specific. The IACP recommends that communities be actively involved when law enforcement considers utilizing drones. These guidelines also include system requirements, and discuss procedures for transparency and safety, as well as discouraging equipping drones with weapons and enhanced technologies. In regards to Operational Procedures, the recommended guidelines discuss the procedures used to acquire a drone and how the use of that drone should be kept transparent. The focus is on transparency through audits and using "Reverse 911" to alert those living and working in the vicinity of deployed home. The operational procedures also address when a warrant is required, although only in broad terms, and is more useful as a general principle than clear law enforcement guidelines.

C. **Jay Stanley and Catherine Crump, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*, AM. CIVIL LIBERTIES UNION, Dec. 2011.**

This Report is helpful to understanding the major privacy concerns and also acknowledges the issue of enhanced technology capable of being used by drones. The ACLU Report begins by discussing what a drone is and different kinds of drones. The Report then identifies different types of advanced surveillance technology that drones can use such as high power lenses and video analytics. This may be useful in identifying the types and concerns of enhanced technologies drones are capable of utilizing. The Report lists several privacy concerns including some that may affect First Amendment Constitutional rights, which may be useful to assess ACLU privacy concerns. The report goes on to address Fourth Amendment and drone use. The ACLU argues that while there are no Fourth Amendment cases which take a position on the use of drones specifically, courts should scrutinize drones which carry enhanced technology. The Report addresses the following cases: *CA v. Ciraolo* (flying in public airspace), *Dow Chemical Co. v US* (use of advanced camera to take photos from the air), *FL v. Riley* (flying helicopter in public airspace), and *US v. Knotts* (ACLU discusses language regarding prolonged surveillance). The ACLU finally makes recommendations including usage restrictions, image retention restrictions, public notice, democratic control, and auditing.

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure

The Mesa County Sheriff's Office Unmanned Aircraft Operations Manual

DRAFT

Jan 2015

PREFACE

The following procedures are intended to promote the safe and efficient operation of the department's unmanned aircraft. **SAFETY**, **above all else, is the primary concern in each and every operation, regardless of the nature of the mission.**

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

MISSION STATEMENT

It shall be the mission of those personnel of the Mesa County Sheriff's Office to be trained in the use of unmanned aircraft systems to use this resource to protect the lives and property of the citizens of Mesa County and to prevent and detect crime

To provide air support in locating and apprehending wanted subjects, missing persons and for other search and rescue missions. Further, to aid in the adjudication of cases. Finally, to perform any task that can best be accomplished from the air in an efficient and effective manner with all due regard to the protections of the Constitution of the United States of America and the State of Colorado.

DRAFT

01.00.00 ADMINISTRATIVE MATTERS

01.01.00 UNMANNED AVIATION OPERATIONS MANUAL

01.01.01 The guidelines contained in this manual are issued by authority of the Sheriff. As such it is an official document of the agency.

01.01.02 The manual is not intended to be all-inclusive, but as a supplement to other department policies, Federal Aviation Regulations, aircraft manufacturers' approved training, etc.

01.01.03 This manual has been written to address unmanned aircraft operations as they existed when it was drafted. Equipment, personnel, environment (internal and external), etc., change over time. The management of change (MOC) involves a systematic approach to monitoring organizational change and is a critical part of the risk management process. Given this, it is essential that this manual be continually updated as necessary. The entire manual will be reviewed annually to assure it is up to date. Any changes to the manual will be communicated immediately to all members.

01.01.04 A copy of the manual (electronic or paper) will be issued to every member having unmanned aircraft responsibilities.

01.02.00 ORGANIZATION

01.02.01 Unmanned Aviation operations shall be comprised of those personnel assigned by the Sheriff and includes operators, observers and others deemed necessary.

01.02.02 Aviation operations are under the direct command of the Operations Lieutenant.

01.02.03 Personnel assignments can be on a full-time, part-time, extra duty or volunteer.

01.03.00 PERSONNEL

01.03.01 Commanding Officer - The Operations Captain serves as the commanding officer of unmanned aviation operations and is responsible for overall management and supervision of the operation, which includes budget preparation and control, personnel selection, etc.

1. Given the technical nature of aviation, the Captain may, at their discretion, assign responsibility for unmanned aviation operations to any member who has the knowledge, skills and abilities to safely and effectively manage the operation.

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

01.03.02 Supervisor

1. The Captain may assign a subordinate to serve as the supervisor of unmanned aviation operations.
2. At the discretion of the Captain, one UAS team member may be designated as the supervisor of aviation operations. Normally this will be an operations Lieutenant.

01.03.03 Operators

1. To be considered for selection as a operator, applicants must be in good standing with the agency, meet all volunteer requirements and meet any other requirements imposed by the Sheriff.
2. A operator's primary duty is the safe and effective operation of the agency unmanned aerial system in accordance with manufacturers' approved flight manual, FAA regulations and agency procedures. Pilots must remain knowledgeable of all FAA regulations; aircraft manufacturer's flight manual and sheriff's office policies and procedures.
3. Operators may be temporarily removed from flight status at any time by the Sheriff, or their designee, for reasons including performance, proficiency, etc. Should this become necessary, and the operator will be notified.

01.04.00 MISCELLANEOUS

01.04.01 Inquiries from the news media will be forwarded to the PIO for response.

01.04.02 Requests for support from other government agencies within, or outside Mesa County shall be forwarded to the Sheriff, operations Captain, Program Manager or supervising operations lieutenant for consideration.

01.04.03 Complaints about aircraft operations shall be referred to the Professional Standards Unit.

02.00.00 SAFETY

02.01.00 SAFETY POLICY

02.01.01 The Sheriff is committed to having a safe and healthy workplace, including:

DRAFT

1. The ongoing pursuit of an accident free workplace, including no harm to people, no damage to equipment, the environment and property.
2. A culture of open reporting of all safety hazards in which management will not initiate disciplinary action against any personnel who, in good faith, disclose a hazard or safety occurrence due to unintentional or intentional conduct.
3. Support for safety training and awareness programs.
4. Conducting regular audits of safety policies, procedures and practices.
5. Monitoring the unmanned aviation community to ensure best safety practices are incorporated into the organization.

02.01.02 It is the duty of every agency member with unmanned aviation responsibilities to contribute to the goal of continued safe operations. This contribution may come in many forms and includes always operating in the safest manner practicable and ***never taking unnecessary risks***. Any safety hazard, whether procedural, operational, or maintenance related should be identified as soon as possible after, if not before, an incident occurs. Any suggestions in the interest of safety should be made to the operations Captain without reservation.

02.01.03 If any member observes or has knowledge of an unsafe or dangerous act committed by another member, the operations Captain is to be notified immediately so that corrective action may be taken.

02.02.00 UAS Program Manager

02.02.01 The Program Manager is responsible for the following:

1. Ensuring all flight operations personnel understand applicable regulatory requirements, standards and organizational safety policies and procedures.
2. Observe and control safety systems by monitoring and supervision of operators.
3. Measure operator performance compliance with organizational goals, objectives and regulatory requirements.
4. Review standards and the practices of agency personnel as they impact flight safety.

02.02.00 SAFETY OFFICER

02.02.01 One member may be designated as the safety officer. This assignment will be in addition to other duties.

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

02.02.02 Duties of the safety officer may include:

1. Copy and circulate pertinent safety information.
2. It is emphasized again that safety is the responsibility of ALL members, not just the safety officer.

02.03.00 SAFETY TRAINING

02.03.01 All new members shall receive training in the following prior to serving in an operational capacity:

1. Agency commitment to safety.
2. Agency policy/SOP.
3. The member's role in safety.
4. Process for reporting hazards and occurrences.
5. Applicable emergency procedures.

02.04.00 SAFETY STAND DOWN

02.04.01 A safety "stand down" will be conducted annually. During a stand down, all members with unmanned aviation responsibilities assemble to review the agency safety program. It is also an opportunity to solicit changes to this manual, identify potential hazards, update emergency notification forms, conduct safety training, etc. The length of the meeting is dependent on the needs of the agency.

02.04.02 During the stand down meeting, normal operations are suspended to assure that all members are focused on the safety of the program.

02.05.00 MEDICAL FACTORS

1. Each member shall report to duty rested and emotionally prepared for the tasks at hand.
2. Physical illness, exhaustion, emotional problems, etc., can seriously impair judgment, memory and alertness. The safest rule is not to act as a flight crew member when suffering from any of the above.
3. A self-assessment of physical condition shall be made by all crew members during preflight activities.
4. No member shall act as an crew member within eight hours after consumption of any alcoholic beverage, while under the influence of alcohol, or while having an alcohol concentration of 0.04 or greater in a blood or breath specimen (FAR 91.17).

DRAFT

03.00.00 TRAINING

03.01.00 OBJECTIVE

1. The key to continued safe operations is by maintaining a professional level of unmanned aviation competency. The first step in this process is establishing minimum qualifications for selecting aircrew. The second step involves training.

03.02.00 INSTRUCTORs

1. The Program Manager will designate instructors who will organize proficiency exercises as well as on going training.

03.03.00 TRAINING PLANS

1. All members will have a training plan on file that outlines training objectives for the upcoming year.
2. The approved training plan will be developed jointly by the Program Manager, supervisor lieutenant, instructors and team members, as appropriate.
3. Training objectives will vary depending on whether the member is new to unmanned aviation or an existing member. For new members, the focus will be familiarization with the equipment and operational procedures. Existing members will focus on recurrent training etc. Objectives should challenge the member to increase their competency in the knowledge and skills necessary to perform.
4. Training plans shall be maintained in a file and reviewed monthly to assure progress towards objectives.

03.04.00 INITIAL TRAINING

1. Initial training will be conducted to provide new operators with skills sufficient to operate unmanned systems, including specific system training.
2. New operators need to become familiar with aviation operations, the unmanned aircraft and its equipment.
3. Any new member who fails to successfully complete initial training may be subject to removal from the team.

03.05.00 RECURRENT TRAINING

1. In any case, regular proficiency flights will required for each individual operator. Proficiency is defined as being able to consistently demonstrate a level of skill in operating unmanned systems.

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

2. Any pilot who has not flown an unmanned aircraft of the type operated by the sheriff's office for 30 days or longer must successfully complete a proficiency flight prior to acting as pilot in command of agency aircraft.
3. Recurrent training is not limited to actual operator skills but includes knowledge of all pertinent unmanned aviation matters.
4. Failure to prove proficiency can result in removal from unmanned aviation responsibilities.

03.08.00 USE OF SHERIFF'S OFFICE UNMANNED AIRCRAFT FOR TRAINING

1. Agency aircraft can be used to meet the training objectives set forth in the member's training plan.

04.00.00 GENERAL OPERATING PROCEDURES

04.01.00 REQUESTS FOR UNMANNED AIRCRAFT SERVICES

1. Requests received during duty hours will be handled by the on duty team member. If no member is on duty the supervising operations Lieutenant and/or the program manager will be contacted.
2. Requests for immediate assistance during non-duty hours will be referred to the on-call crew by the Regional Communications Center who will maintain an up to date on-call list.
3. Requests during non-duty hours that are not of an immediate nature will be referred to the patrol supervisor.

04.02.00 MISSION PRIORITIES

1. Several requests for unmanned aircraf services may be received simultaneously. Given the limited number of unmanned aircraft and personnel available, it is necessary to prioritize calls for service.
2. In general terms, calls are prioritized as follows (listed in order of importance):

    - In-progress calls involving a threat to the safety of any person
    - Search and rescue of innocent victims
    - Searches for fleeing criminal suspects
    - Crime in progress calls
    - Crime Scene reconstruction operations
    - Traffic control operations
    - Requests to support other government agencies

04.03.00 FLIGHTS LEAVING THE COUNTY

DRAFT

1. Planned flights leaving the jurisdictional boundaries of MESA COUNTY need the specific approval of the Sheriff/Designee and may require specific FAA authorization.

04.04.00 FLIGHT CREW RESPONSIBILITIES

1. Operator in Charge (OIC)

   - The OIC is directly responsible for and is the final authority over the operation of the unmanned aircraft.
   - OICs have absolute authority to reject a flight based on weather, aircraft limitations, physical condition, etc. No member of the Sheriff's Office, regardless of rank, can order an operator to make a flight when, in the opinion of the OIC, it cannot be done safely.
   - OICs are responsible for compliance with this manual and Federal Aviation Regulations.
   - OICs shall handle radio communications with air traffic control and other aircrafts.
2. Sensor operator/Observer (S/O)

   - The S/O is responsible for the law enforcement aspect of the mission and must be a member of the UAS team.
   - The S/O shall operate the payload and handle radio communications between ground units and dispatcher.
   - The S/O shall remain alert for suspicious persons or activities on the ground and coordinate response by ground units.
   - The S/O will avoid unnecessary communications with the OIC during takeoff and landing.

3. Observers
   - Observers are to assist the OIC with situational awareness of the airspace and can be designated from any member of the Sheriff's office by the OIC on scene.

4. Crew Coordination

   - The OIC and S/O will work together to form the crew which will ultimately accomplish mission objectives.
   - In the interest of safety, both the OIC and S/O must be comfortable with any decision made while working as a crew. This begins when deciding whether to accept a mission and continues throughout the mission. If there is genuine concern on the part of either the OIC, or S/O, the mission should not be accepted or should be terminated.

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

- Concern on the part of either crew member should be immediately expressed to the other member. Communication is the key. Many times, reservations about something can be put to rest with a simple explanation.
- S/O's have the right, as well as the responsibility, to question the OIC whenever they do not understand something, or are uncomfortable with certain procedures, weather, etc. Conversely, the OIC should honestly answer any questions posed to them and not feel as though he/she is being challenged, or threatened.
- THE CREW CONCEPT AND OPEN COMMUNICATION WILL HELP ACHIEVE SAFE OPERATIONS.

04.06.00 FLIGHT TIME LIMITATIONS AND REST REQUIREMENTS

04.06.01 During any 24 consecutive hours, the total flight time of any OIC may not exceed 8 hours. A OIC flight time may exceed the flight time limits if the assigned flight time occurs during a regularly assigned duty period of no more than 14 hours and:

04.06.02 Each flight assignment under 04.06.01 must provide for at least 8 consecutive hours of rest during the 24-hour period that precedes the planned end of the agency flight.

04.07.00 PERSONAL PROTECTIVE EQUIPMENT

04.07.01 Other

1. Service weapons/Duty gear may be worn/carried by Mesa County Sheriff's Office UAS Team members authorized to carry such weapons.

04.08.00 PREFLIGHT ACTIONS

04.08.01 Thorough preflight planning and inspections are critical to safe operations.

04.08.02 Physical Assessment

1. Preflight begins with the crew making a self-assessment of their physical condition.
2. If unable to perform flight duties, the crew member will decline such activity.

DRAFT

04.08.03 Inspections

1. At the beginning of each flight, the OIC shall conduct a thorough preflight inspection of the unmanned aircraft in accordance with the instructions contained in the unmanned aircraft flight manual.
2. It has been recognized that the use a checklist is a major weapon in combating aviation accidents. Checklists will be utilized.

04.08.04 Weather

1. At the beginning of each flight, the OIC check the weather. The OIC will ensure that he/she gathers enough information to make themselves familiar with the weather situation existing throughout the area of operation.
2. Subsequent to the original weather check, OICs will obtain, as necessary, sufficient weather information to ensure that the original check stays valid. The frequency of these additional weather checks will be determined by the severity of existing or forecast weather.

04.08.05 Documentation

1. All unmanned aircraft flights will be logged.
2. Documentation will be maintained in file for a period of, at least, one year.

04.08.06 Preflight Planning

1. The OIC shall familiarize themselves with all available information concerning the flight.

04.09.00 GROUND HANDLING

1. The OIC is responsible for operation of the unmanned aircraft in the air and on the ground. OIC will ensure that no unauthorized items are attached to the aircraft prior to movement. During movement, adequate clearance will be maintained.
2. Upon "Repack" of the unmanned aircraft the Pilot will ensure that all items are returned to their proper place.

04.10.00 POST FLIGHT RESPONSIBILITIES

1. A thorough inspection will be conducted of the unmanned aircraft immediately after the completion of the mission to ascertain if any damage was sustained during operation.
2. If necessary, the unmanned aircraft will be serviced so that it is immediately available for the next flight.
3. Necessary entries will be made into the aircraft flight log and appropriate reports will be completed.

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

04.11.00 EMERGENCY RESPONSE PLAN

04.11.01 During unmanned aircraft operations, emergency situations may develop at any time. The primary concern in such incidents is the prevention of injury to persons on the ground and/or other users of the National Airspace. Secondary concerns include protection of property and non living entities on the ground.

04.11.02 For an unmanned aircraft accident with personal injury and/or significant property damage, the crew (if able) shall do the following:

1. Immediately notify dispatch and request assistance. Provide as much information as possible about the extent of the injuries, or damage.
2. Provide information to Air Traffic Control as necessary.
3. Render first aid to the injured.
4. Request notification of the supervisor/Program Manager and Sheriff, who will respond to the scene and coordinate accident investigation efforts.
5. Request the FAA and NTSB be notified if necessary.
6. Survey the damage to the unmanned aircraft and/or other property.
7. Provide any additional assistance or information requested by the FAA and NTSB.
8. Submit a detailed, written report to the Sheriff.

04.11.03 For ground emergencies, personnel shall:

1. Evaluate the need for response by FIRE or EMS.
2. Provide first aid, contain the incident, etc.
3. Notify the supervisor/program manager and Sheriff.

04.11.04 Pre-Planning for Emergencies

1. Safety response training will be conducted annually.
2. All members should receive basic first aid training.

04.15.00 MISCELLANEOUS

04.15.01 Personal use of Sheriff's Office unmanned aircraft is prohibited.

DRAFT

05.00.00 UNMANNED AIRCRAFT OPERATIONS

05.01.00 GENERAL – Unmanned Aircraft will be operated in accordance with this manual, Federal Aviation Regulations and the manufacturer's manual.

05.02.00 FLIGHT LIMITATIONS

05.02.01 Weather

1. Flight into instrument meteorological conditions, thunderstorms, or other severe weather is prohibited.
2. No aircraft operations will be conducted when the ceiling is less than 500' AGL.

05.02.02 Maximum Altitudes

1. The maximum altitude for operations is 400' AGL.

05.02.03 Miscellaneous

1. Should the OIC or S/O develop fatigue or a sudden illness, the flight shall be terminated as soon as practical.

05.03.00 GROUND SAFETY

1. The OIC and S/O must be constantly aware of dangers to ground personnel.
2. The OIC will not under any circumstances leave any unauthorized person in charge of the unmanned aircraft controls.

06.00.00 MAINTENANCE

06.01.00 GENERAL

1. Properly maintained unmanned aircraft are essential to safe operations. Compliance with manufacturer's scheduled maintenance, preflight inspections and immediate repair of mechanical problems ensure the availability and safety of agency unmanned aircraft.

06.02.00 DEFINITIONS

1. **Aircraft Flight Log –** Flight record book.

DRAFT

Mesa County (Colorado) Sheriff's Office UAS Standard Operating Procedure, continued

2. **Preventive Maintenance** – Simple, or minor preservation operations or the replacement of small standard parts not involving complex assembly operations.
3. **Scheduled Maintenance –** Periodic maintenance on aircraft at known intervals.
4. **Unscheduled Maintenance –** Repairs to aircraft in response to mechanical deficiencies.

06.03.00 RESPONSIBILITIES

06.03.01 Maintenance Officer

1. One member will be designated as the maintenance officer who will coordinate maintenance for agency unmanned aircraft. This assignment will be in addition to other duties.
2. If possible, maintenance will be scheduled when it will have the least impact on operations.
3. The maintenance officer shall maintain the aircraft.
4. The maintenance officer supervisor/program manager and Sheriff shall prepare the annual budget request for maintenance related needs. To do so, it will be necessary to accurately project which life-limited parts, or calendar-life components will need to be replaced, which systems require certification, required inspections, etc.

06.03.02 Operators in Charge

1. Conduct a thorough preflight inspection of the unmanned aircraft in accordance with the unmanned aircraft flight manual.
2. The Aircraft Flight Log shall be reviewed prior to flight and the appropriate data entered at the conclusion of each flight.
3. In accordance with the Federal Aviation Regulations (refer to FAR Part 43.3), pilots can perform preventive maintenance
4. The OIC is the final authority on whether an aircraft is airworthy.

DRAFT

APPENDIX 13

Arlington (Texas) Police Department UAS Standard Operating Procedure

108.00 AVIATION UNIT (ADDED 3-27-13)

A. **Purpose and Philosophy**

The Arlington Texas Police Department has implemented a small Unmanned Aircraft System ("sUAS") program to assist law enforcement by providing increased situational awareness, enhanced officer safety, and act as a force multiplier to improve operating efficiency. This policy sets forth how the sUAS program will operate the aircraft in coordination with law enforcement officers conducting a specific mission as guided by the Certificate of Authorization (COA) issued by the Federal Aviation Administration (FAA). This policy is designed to minimize risk to people, property, and aircraft during the operation of the sUAS while continuing to safeguard the right to privacy of all persons.

B. **Definitions**

1. *Special Operations Commander* - The individual responsible for reviewing and approving the use of the sUAS in a law enforcement mission. The Special Operations Commander has full oversight responsibility of all logistical and administrative elements of sUAS operations.

2. *Team Leader* – The individual responsible for assisting the Special Operations Commander with administrative functions related to the sUAS program, including maintaining a current list of all equipment that could be placed on the sUAS during operations. The Team Leader is also responsible for the condition and maintenance of the sUAS. (A 41.1.3c & d) (Revised 05-23-13)

3. *Assistant Team Leader* – The individual responsible for assisting the Special Operations Commander and Team Leader with administrative functions related to the sUAS program.

4. *Pilot in Command* (PIC) – The individual responsible for the overall flight operations of a specific mission.

5. *Observer* – The individual trained to maintain the line-of-sight and 360 degree hazard awareness around the sUAS at all times and assist the PIC in carrying out all duties required for the safe operation of the sUAS.

6. *Camera and Remote Sensing Operator* - The individual responsible for the operation of all camera (video and still) and remote sensing functions during sUAS operations.

7. *Defined Incident Perimeter* - a location identified via a Very High Frequency Omnidirectional Range (VOR) Radial/Distance Measuring Equipment (DME) fix. The location has a defined perimeter to be determined based on the scope of the operation and a defined operational ceiling at or below 400 feet Above the Ground (AGL).

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

8. *Pre-Flight Briefing* – a discussion led by the PIC prior to aircraft launch which shall include but not be limited to:
   a. Review of mission goals and methods to achieve goals, including handoff procedures.
   b. Review of current and forecasted weather conditions and weather limitations on mission.
   c. Review of current Notice to Airmen (NoTAMs) and Temporary Flight Restrictions (TFRs) that have been issued for the proposed flight area.
   d. Identification of mission limitations and safety issues such as battery charge, GPS strength, and potential for radio interference.
   e. Review of proposed flight area, including maximum ceiling and floor.
   f. Review of communication procedures between PIC, Observer, Camera Operator, and other ground support, including the availability of two cell phones to communicate with Air Traffic Control in the event of a fly-away or other flight emergency.
   g. Review of emergency/contingency procedures including aircraft system failure, flight termination, divert, and lost link procedures.
   h. Review of required video or digital images.
   i. Contents of the COA
   j. Frequencies to be used.
   k. Execution of a pre-flight check following the approved checklist.

C. Aircraft

1. General Airworthiness. The Special Operations Commander shall be responsible for ensuring that the sUAS is maintained and flight ready according to the manufacturer's recommendations and related industry standards. In addition, the Special Operations Commander may rely upon the testing data and evaluation data provided by other government agencies, the aircraft manufacturer, and independent testing facilities.

2. Mission Specific Airworthiness. The PIC shall be responsible for ensuring that the sUAS is airworthy prior to each mission. The PIC may rely upon the inspection and reports provided by agency personnel appointed with the responsibility for maintaining the sUAS.

3. Radio Frequency. The sUAS shall use the assigned radio frequencies and antenna equipment approved in the most current COA issued by the FAA.

4. Maintenance. The Team Leader is responsible for the maintenance of the sUAS, which shall be performed by Aviation Unit pilots specifically trained on the maintenance of the sUAS or by manufacturer certified representatives and personnel. The PIC and/or Observer shall perform a pre-flight and post-flight inspection of the sUAS. Any equipment issues (otherwise known as squawks) shall be entered in the aircraft's squawk log and immediately reported to the

Special Operations Commander. It shall be the responsibility of the Special Operations Commander to determine whether the reported squawks or issues need to be corrected prior to the next flight, which will then be documented in the aircraft's squawk log. (A 41.1.3c) (Revised 05-23-13)

5. Software and hardware changes. All changes shall be documented in the unmanned aircraft and ground control station logbooks by persons authorized to conduct UAS maintenance. All previously proven systems, to include payloads, may be installed or removed as required for missions and documented in the appropriate aircraft squawk log. Test flights must be conducted and documented after major changes in the hardware or software.

6. Storage Transport. The aircraft shall be stored in a secure manner to limit possible damage to the unit while in transit. The blades are to be folded into the blade holder on the boom of the helicopter and the full helicopter should be stored in the assigned aircraft case. The case top should be installed directly down on top of the helicopter and all latches secured prior to transport. Batteries must be transported in an appropriate container to prevent possible damage to the batteries. Batteries should not be dropped or punctured.

7. Battery Charge. Any components necessitating a charged battery shall be charged in accordance with manufacturer's recommendations. To the extent permissible by manufacturer's recommendations, the sUAS shall be fully charged when not in use. The Lithium-ion Polymer (LiPO) batteries should be charged and stored in a cool and dry location. Because of the fire hazard risk, batteries should not be left unattended when charging at full or rapid charge (vs. trickle charging) and should be charged at the recommended amperage and not exceeded. If the LiPO batteries begin smoking or expanding (puffing) they should immediately be isolated for risk of explosion or fire. Never completely discharge LiPO batteries or they will become un-useable (i.e. unable to hold a charge).

D. Pilots (A 41.1.3b)

1. Pilot Rating. PIC's flying in Class D airspace or night operations (when approved) must hold, at a minimum, a FAA Private Pilot Certificate or a FAA accepted military equivalent; currency in a manned aircraft is not required. PIC's flying in Class G or E airspace only must have a current certificate indicating successful completion of the Private Pilot written exam.

2. Initial Training. All pilots who will be flying law enforcement missions shall be properly trained by either manufacturer representatives or Certified Instructors as designated by the manufacturer. The sUAS pilots will meet all conditions of the (COA) issued by the FAA, including a current Second Class Medical Certificate or equivalent. The pilots will have a current working knowledge of the airspace intended for operations, Air Traffic Control communication requirements, specific sUAS aerodynamic factors, and the ability to obtain and interpret weather. All

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

pilots must meet the following flight experience requirements and be current with their flight log entries.

1. Basic Flight Operations Training. Once the pilot has passed the written private pilots exam and Second Class Medical as required by FAA guidelines, all pilots must successfully complete and pass the Basic Flight Operations Training/Curriculum for sUAS as approved in consultation with the manufacturer.
2. Mission Training. All pilots must undergo Mission Training to increase specific core competencies in all sUAS operations, systems and roles with conducting a mission in accordance with approved Mission Training Curriculum. This training is in addition to Basic Flight Operations Training.

3. Currency Training. All pilots must have a minimum of three qualifying sUAS flights to include take-offs and landings in the preceding 90 days to be eligible to fly sUAS missions.

   a. In order to accomplish required currency training, pilots shall participate in 16 hours (two days) of monthly training, at a minimum, as assigned by personnel order.

   b. Recurrent training is not limited to actual pilot/observer skills, but includes knowledge of all pertinent sUAS and aviation matters.

   c. All members within the sUAS unit shall read the current COA and maintain proficiency in their operator/observer abilities. Members who do not have documented training or flight time for the preceding 90 days shall demonstrate proficiency before performing pilot/observer duties during a mission.

   d. Failure to maintain/prove proficiency can result in removal from sUAS operations.

4. In-service Training. Each pilot must undergo in-service training every 12 months to include updated industry standards and field exercises, as well as a review of current case law governing the use of aviation assets as designated by the Special Operations Commander.

E. Observer. An Observer is required for all practice and mission flights of the sUAS.

1. Initial Training: sUAS Observers shall meet all conditions of the most recent COA issued by the FAA. Observers will have a current working knowledge of the airspace intended for operations, Air Traffic Control phraseology and communication requirements, specific sUAS aerodynamic factors, and the ability to obtain and interpret weather. The Observer will receive specific training on relevant Part 91 regulations (14 CFR Part 91-Code of Federal Regulation), such as the obligation to see and avoid other aircraft and the ability to identify position for purposes of relaying position reports to the PIC. (A 41.1.3b)

2. Pre-flight Briefing: Observers must participate in the pre-flight briefing.

F. Camera and Remote Sensing Operator

1. Initial Training: The Camera Operator will receive specific training on camera and sensing equipment operations, including recording and storing digital data for evidentiary purposes prior to assisting with mission flights. (A 41.1.3b)

2. Pre-flight Briefing: Camera Operators must participate in the pre-flight briefing.

G. Flight Conditions (41.1.3a)

1. Daylight: All sUAS operations shall be conducted during daylight. Night flight is prohibited unless specifically authorized by the FAA in an Emergency COA.

2. Line-of-sight: All sUAS operations shall be conducted within line-of-sight of the PIC or Observer such that the Pilot or Observer may detect and avoid hazards such as aircraft and property.

3. Altitude: All flights shall be conducted at less than 400 feet Above Ground Level (AGL), unless otherwise noted in the COA or approved by FAA in an Emergency COA. All flights will be conducted under VFR (Visual Flight Rules) for Class E weather conditions.

4. Weather: The PIC is responsible for obtaining current weather reports from an appropriate source as denoted in the Aeronautical Information Manual (AIM). This includes calling the closest airport with Automated Weather Observation Systems (AWOS) or Automated Terminal Information System (ATIS) and calling the Flight Service Station (FSS) for a weather report for the area of operations. A standard Meteorological Terminal Aviation Routine report (METAR) and Terminal Aerodrome Forecast (TAF) report shall be obtained regardless of visibility. Flight operations are not authorized in known icing conditions as defined in 14 CFR 91.

H. Operating Guidelines (A 41.1.3a)

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

1. Heat: The operational guidelines for heat are less than 110 degrees Fahrenheit (37.77 degrees Celsius) at ground level. Operation in temperatures over this mark should be noted with the air density as obtained from the pre-flight weather report. The battery and length of flight should be adjusted accordingly based upon high humidity and temperature with air density. These local conditions may warrant the PIC opting to not fly based upon these flight conditions.

2. Cold: The operational guidelines for cold are greater than 0 degrees Fahrenheit (-17.77 degrees Celsius) at ground level. Operation in temperatures under this mark should be noted with the air density as obtained from the pre-flight weather report. The battery and length of flight should be adjusted accordingly. Also, if the moisture level is high, conditions should be noted for icing on wings and flight surfaces. These conditions may warrant the PIC opting to not fly based up these flight conditions.

3. Wind: The sUAS will not be operated in sustained winds greater than 30 knots (35 mph). Wind velocity can be obtained from a hand-held anemometer used at the training location or mission site. General weather information can be obtained from the ATIS and FSS. The PIC may decide that wind conditions at the area of operation are too hazardous and opt to not fly.

4. Rain, Snow and Fog: The operational guidelines for these conditions are based upon visibility and operator safety at the local site. The PIC and Observer must adhere to the line-of-sight and VFR weather minimum requirements.

I. Flight Requirements

1. Mission Requests. All requests for sUAS to provide support for a mission shall be forwarded to the Special Operations Commander. Considerations for use of sUAS shall include the following:

    a. the location of the mission, for purposes of insuring the safety of people and property.
    b. the intended area of operation, for purposes of evaluating the ability to mitigate potential air-to-air conflicts. Such evaluation will consider the current landing patterns at airports in the vicinity. Whenever the approach path of an airplane to a nearby airport would involve flying over the intended area of operation, such operations shall be coordinated with the appropriate air-traffic control facility. All coordination will be done in accordance with any requirements in the police department's COA issued by the FAA.

c. The weather and its potential affect on the aircraft, including the potential to carry the aircraft to an area of air-to-air conflict.
d. The currency of the PIC and Observer.
e. The potential usefulness of the information gathered by the sUAS versus information gathered through other means.
f. Any other relevant risk factors to successfully complete a risk benefit analysis for the use of sUAS in the specific mission. Risk factors may include but are not limited to tree canopy, distance between buildings, smoke, etc.
g. Strength of radio and GPS signal as indicated on the sUAS.

2. Personnel Designation. Once the Special Operations Commander has approved the mission request, the Commander shall identify the PIC, Observer, Camera Operator, and person responsible for controlling access to the take-off and landing site and coordinate with individual(s) requesting the mission. (A 41.1.3a)

3. Pre-flight Preparation. Before any mission the PIC must conduct a Pre-Flight Briefing.

4. Scene Review. The PIC and Observer are responsible for identifying any unsafe conditions at the scene. This includes, but is not limited to:

a. Take-off and landing site: This area should be free of obstructions, items on the ground and debris that may interfere with the rotors. This includes creation of a flight line, from which other law enforcement officers and civilians must remain clear.
b. Flight perimeter: The site must utilize law enforcement officers and standard protocols to minimize civilian traffic or interference during the operation.
c. Safety View: The flight team should identify trees, bushes, power lines, and other potential obstructions and coordinate the pre-flight briefing accordingly.
d. Interference: The flight team should identify Cell Towers, TV and Microwave sources, which might create interference with the flight equipment. The equipment should be tested on the ground to insure proper communications and operation before the flight.
e. Sectional chart: The flight team will maintain a current copy of a VFR Sectional Chart for the area in which flight operations will occur.

5. Notice to Airmen (NoTAM). A distance (D) NoTAM shall be issued for all sUAS training and mission operations through the local NoTAM issuing authority at the DFW Flight Service Station (FSS).

6. TRACON (Terminal Radar Approach Control) notification. The PIC (or designee) shall notify the Dallas/FW TRACON at least 30 minutes prior to operation. Such notification should include the following:

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

a. The intended location, time and duration of the flight.
b. The maximum altitude of the flight.
c. NoTAM number.
d. A cell phone number of an individual for emergency contact.
e. The PIC (or designee) shall provide flight notification to any other entities required in the COA, e.g., Bell Helicopter.
f. The PIC shall immediately notify TRACON, Air Traffic Control of Arlington or Grand Prairie and any others previously notified immediately at the conclusion of the sUAS flight.

7. Coordination with Air Traffic Control (ATC). The PIC/Observer will maintain direct, two-way communication with the Arlington or Grand Prairie ATC and have the ability to maneuver the sUAS in response to ATC instructions.

   a. The PIC must not accept ATC instructions that require visual separation from the sUAS.
   b. ATC may assign a radio frequency for air traffic during the flight.
   c. ATC may provide a written waiver of two-way communication.

8. Documentation. A copy of the current COA, flight log, squawk log, and Pilot Certifications must be kept with the sUAS at all times. PIC's and Observers must be in possession of their Second Class Medical Certificates at all times.

9. Flight operations.

   a. All flight operations shall be conducted in accordance with the manufacturer's recommendations.
   b. The sUAS must operate with position/navigation or anti-collision lights at all times unless authorized by the FAA.
   c. If at any time the PIC and/or Observer believe there is a potential for air-to-air conflict, risk of harm to individuals or property, the PIC shall immediately land the aircraft.
   d. In the event of lost communications with the aircraft, lost link procedures shall be executed including immediate landing of the aircraft. If the aircraft does not immediately execute these orders, the PIC shall notify the appropriate ATC. If the PIC loses visual contact, ATC shall be immediately notified.

10. Emergency Exceptions. An application for an Emergency COA must have prior approval from the Special Operations Commander before being submitted to the FAA.

J. Prohibited Acts (A 41.1.3a)

1. Warrantless Search: The sUAS shall not be operated in violation of the Texas and United States constitutions, statutes, or regulations. When a search warrant is required by law and no warrant exception exists, flight is prohibited unless a search warrant signed by an authorized magistrate is obtained.

2. Routine Patrol: sUAS shall not be used for routine patrol duties.

3. Exceeding Aircraft Limitations: The sUAS shall not be flown in conditions that exceed the manufacturer's recommended limitations, including range, ceiling, wind strength, and battery charge.
4. High Risk Missions: The sUAS shall not be flown for any mission in which the Special Operations Commander or the PIC determines the risk of flying the sUAS outweighs the benefit to the mission. Risks may include hazards to individuals or property on the ground, possible collision hazard with other aircraft, loss of control of the sUAS. The Special Operations Commander cannot countermand a PIC's determination to not fly a mission. However, the Special Operations Commander can countermand a PIC's determination to fly a mission. The PIC has sole accountability for the sUAS during flight operations.
5. Spraying and Dropping: The PIC is prohibited from spraying or dropping anything from the aircraft and carrying hazardous materials.

6. Prohibited Airspace: sUAS flights are prohibited in Class B airspace, located generally above Interstate 30. Flights in Dalworthington Gardens, the City of Pantego, and areas outside Arlington city limits are prohibited, unless specific authorization is received from the FAA.

7. Defined Incident Perimeter: Unless authorized by the FAA only one sUAS shall be operated in a defined incident perimeter, by a single control station, and by one pilot at a time.

8. Daisy-chaining Observers: Unless authorized by the FAA, daisy-chaining Observers to extend line-of-sight is prohibited.

9. Manned Aircraft in Operating Area: sUAS flights are prohibited when other manned aircraft are operating within the defined incident perimeter.

10. Flying for Compensation: As a "public aircraft," flying for compensation or hire is prohibited. Cost reimbursement between government units is permitted.

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

K. Documentation and Reporting

1. Flight Documentation. The PIC or their designee shall complete all department flight documentation including pertinent information about the aircraft, flight conditions, type of mission, and mission parameters. Monthly reports containing the above information or indicating no flights occurred during the month shall be submitted to the FAA through the COA online system by the APD employee authorized by the FAA to submit the documentation.

2. Incident and Crash Documentation. The Special Operations Commander shall be responsible for reporting any incidents or crashes to the FAA through the COA online system and supplying any additional documentation that may be required.

APPENDIX

PRE-FLIGHT MISSION CHECKLIST

1. **Check METAR and TAF**
    - Winds less than 30 knots
    - Less than 110 degrees Fahrenheit
    - Visibility 3 Statute Miles
    - 1000' ceiling
2. **Issue NOTAM (877.487.6867)**
    - Off the Maverick VOR
    - Identify the radial and distance from Maverick (Nautical Miles)
    - Time of operation (in Zulu)
    - Maximum altitude (400 feet AGL)
    - Record NOTAM # and Briefer's Initials
3. **Mission Brief**
    - Mission objectives
    - Safety parameters
    - Emergency procedures

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

PRE-FLIGHT AIRCRAFT CHECKLIST (Tactical Gimbal)

1. Check Battery Voltage

- Left Main Battery REPEAT/CHECK Minimum 24.5
- Right Main Battery REPEAT/CHECK Minimum 24.5
- Tail Rotor Battery REPEAT/CHECK Minimum 12.0
- Flight Control Batteries (2) REPEAT/CHECK Minimum12.0
- Gimbal Battery REPEAT/CHECK Minimum 12.0

2. Install Batteries

- Left Main Battery CHECK
- Right Main Battery CHECK
- Tail Rotor Battery CHECK
- Flight Control Batteries CHECK
- Gimbal Battery CHECK

3. Gimbal and Video Check

- Check Monitor Voltage CHECK Minimum 10.0
- Mount and Plug in Camera CHECK
- Check Camera Power CHECK Minimum 20 minutes
- Power on JR Video Transmitter CHECK
- Announce Voltage/Unit Number Minimum 9.9
- Connect Gimbal Battery CHECK
- Turn on Gimbal Switch CHECK
- Check RF Light (1) CHECK
- Check Gimbal Controls CHECK
- Turn on Monitor/Camera CHECK
- Check Monitor Display CHECK

4. Check Heli Connections – Mechanical

- Main Rotors CHECK
- Swash Plate Connections CHECK
- Primary Gear CHECK
- Boom Assembly CHECK
- Tail Rotor CHECK
- Landing Gear CHECK

5. Power On JR Heli Transmitter

- Announce Unit # and Voltage CHECK Minimum 10.0
- Switches – Down and Forward CHECK

6. Power on Flight Control

- Connect Flight Control Batteries (2) CHECK
- Switch on Electric Panel CHECK
- Verify Panel Lights Two Blue/Two Green
- GPS Window Acquiring

7. Stick Controls

- Check Stick Controls Manually CHECK

8. Check the Tail Gyro/RF Lights/Balance

- Check Tail Gyro Movement CHECK
- Check RF Lights CHECK
- Check Heli Balance CHECK

9. Connect Batteries (Insure All Connectors "CLICK")

- Left Main Battery CHECK
- Right Main Battery CHECK
- Tail Rotor Battery CHECK
- Ensure Audio Response CHECK

(Observer Verifies ALL Connections)

10. GPS Window

- Check GPS Window Fully Stable

11. Launch Procedure

- Clear Flight Line (Loudly) Clear Flight Line
- Operational Area Clear CHECK

Arlington (Texas) Police Department UAS Standard Operating Procedure, continued

- Timer On CHECK
- Rotor On CHECK

12. Landing Procedures

- Check Timer Announce Time
- Clear Landing Area CHECK
- Check Approach Pattern CHECK
- Safe to Approach CHECK

13. Post Flight Operations

- **DO NOT POWER OFF JR HELI TRANSMITTER**
- Disconnect Main Batteries (2) CHECK
- Disconnect Tail Battery CHECK
- Power off Electrical Panel CHECK
- Disconnect Flight Control Battery CHECK
- Turn off JR Heli Transmitter CHECK
- Power Off Cameral/Gimbal CHECK
- Secure Rotors CHECK
-

14. Debrief Flight/Mission

Complete Flight Log/Squawk Log

APPENDIX 14

Department of Justice Policy Guidance

Department of Justice Policy Guidance[1]

Domestic Use of Unmanned Aircraft Systems (UAS)

INTRODUCTION

The law enforcement agencies of the Department of Justice ("the Department") work diligently to protect the American people from national security threats, enforce our nation's laws, and ensure public safety. In doing so, these agencies use a wide variety of investigative methods. Some of these methods have been in use for decades; others are relatively new and rely on technological innovation. In all cases, investigations and other activities must be conducted consistent with the Constitution and the laws of the United States—and with our commitment to protecting privacy and civil liberties.

In recent years, Unmanned Aircraft Systems (UAS)[2] have emerged as a viable law enforcement tool. UAS have been used to support kidnapping investigations, search and rescue operations, drug interdictions, and fugitive investigations. While they are, in many ways, similar to the manned aircraft that have been in use for many years, they have the potential to provide law enforcement with additional flexibility and yield life-saving benefits. UAS also have the potential to be cost-effective in a time of shrinking government resources. For these reasons, UAS are likely to come into greater use.

As technology advances and enhances our ability to use these new tools, it is important to continue to assess how we use them. A Departmental working group[3] has studied the Department's use of UAS over the last several years and has considered how the technology is likely to evolve in the near future. This policy guidance flows from the working group's discussions and sets forth principles that will apply Department-wide. This policy also applies to

---

[1] This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial or any other proceeding.

[2] "Unmanned Aircraft System" means an unmanned aircraft (an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft) and associated elements (including communication links and components that control the unmanned aircraft) that are required for the pilot or system operator in command to operate safely and efficiently in the National Airspace System. For purposes of this policy, reference to "UAS" includes all onboard sensor equipment.

[3] The Department's working group was led by the Office of Legal Policy and included the Department's Chief Privacy and Civil Liberties Officer and representatives of the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Criminal Division, the Office of Community Oriented Policing, the Civil Rights Division, the Office of the Deputy Attorney General, the Drug Enforcement Administration, the Federal Bureau of Investigation, the National Security Division, the Executive Office for United States Attorneys, the Office of Justice Programs, the Office of Privacy and Civil Liberties, the United States Marshals Service, and the Office of the Chief Information Officer.

Department of Justice Policy Guidance, continued

all instances in which Department components use UAS to support Federal agencies and/or State and Local law enforcement agencies.

This guidance will help ensure that the Department continues to carry out its law enforcement and national security missions while respecting individuals' privacy, civil rights, and civil liberties. It will also help ensure an appropriate level of accountability and transparency. This policy guidance does not replace, and is complementary to, the Federal Aviation Administration rules and regulations that control each and every UAS deployment and help ensure the safe operation of all aircraft, including UAS. This policy guidance is also consistent with the Presidential Memorandum, "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," issued by President Barack Obama on February 15, 2015.

RESPECT FOR CIVIL RIGHTS AND CIVIL LIBERTIES

Respect for civil rights and civil liberties is a core tenet of our democracy. In executing the Department's law enforcement and national security missions, personnel must rigorously support and defend the Constitution and continue to uphold the laws, regulations and policies that govern our activities and operations.

As with all investigative methods, UAS must be operated consistent with the U.S. Constitution. The Fourth Amendment protects individuals from unreasonable searches and seizures and generally requires law enforcement to seek a warrant in circumstances in which a person has a reasonable expectation of privacy. Moreover, Department personnel may never use UAS solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution and laws of the United States. Department personnel may never use UAS to engage in discrimination that runs counter to the Department's policies on race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity. Department personnel must also be trained to understand and abide by all relevant federal legal standards applicable to the use of UAS, and to seek advice from legal counsel as necessary.

In addition, UAS may only be used in connection with properly authorized investigations and activities. Statutory authorities, the Attorney General's Guidelines, and other relevant agency policies and guidance define the scope of authorized investigations and activities and require regular supervisory review and approval. UAS must continue to be used within the context of these existing safeguards.

Further, even within the context of properly authorized activities, personnel often must choose among different investigative methods that are operationally sound, reasonable, and effective, but may be more or less intrusive relative to individuals' privacy and civil liberties. Prior to using UAS, Department personnel must assess the relative intrusiveness of the

proposed use of UAS, and balance it against the particular investigative need.[4] This is both a logical process and an exercise in judgment, but the overall principle remains: in deciding whether to use UAS, Department personnel must consider and, if reasonable based on the facts and circumstances of the investigation, use the least intrusive means to accomplish an operational need.

PROTECTION OF PRIVACY

The Department operates under a set of rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information. For example, the Privacy Act contains provisions on unauthorized use and disclosure of information about individuals, and imposes civil penalties on agencies and criminal penalties on agency personnel for violations of applicable requirements. As with personally identifiable information collected in the course of any investigation, these authorities apply to information collected via UAS. Consistent with applicable existing laws and requirements, the Department's use of UAS shall include the practices identified below.

As noted above, the Department shall only collect, use and disseminate information obtained from UAS for an authorized purpose. The Department shall not retain information collected using UAS that may contain personally identifiable information for more than 180 days unless retention of the information is determined to be necessary for an authorized purpose or is maintained in a system of records covered by the Privacy Act.

Data collected by UAS that is retained must be safeguarded in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. These authorities ensure that Department personnel with access to such data follow practices that are consistent with the protection of privacy and civil liberties. Use of all Department information systems may be monitored, recorded, and subject to audit, and unauthorized collection, retention, or dissemination of data is prohibited. Further, the Department has procedures in place to review, investigate, and address privacy and civil liberties complaints.

Senior Component Officials for Privacy in agencies using UAS must conduct annual privacy reviews of their agency's use of UAS to ensure compliance with existing laws, regulations, and Department policy, and to identify potential privacy risks. They must also, where appropriate, make recommendations to ensure that UAS will continue to be used in a manner consistent with the U.S. Constitution and all applicable laws, regulations, and policies, including those protecting privacy and civil liberties.

---

[4] In assessing the intrusiveness of UAS and the investigative need, personnel must consider factors such as whether the subject enjoys a reasonable expectation of privacy relative to the proposed use of UAS, the scope of the information sought, the scope of the proposed use of UAS, the risk of disclosure to the subject, the seriousness of the crime or national security threat, the strength and significance of the information to be obtained, the efficiency of the method and alternative means available, the amount of information already known about the subject, and the operational security needs of the investigation.

Department of Justice Policy Guidance, continued

ACCOUNTABILITY

The Department promotes accountability by requiring its personnel to accept responsibility for the actions they undertake—and to evaluate the potential consequences of their decisions. The Department imposes codes of conduct to guide employees in the use of all investigative methods, including UAS. As with the use of any technology, there must continue to be mechanisms to hold the Department and its employees accountable.

Part of accountability is ensuring that Department personnel are appropriately trained and supervised. Department personnel whose responsibility it is to manage, supervise, maintain, fly, and/or otherwise use UAS must receive training on this policy and the underlying policies incorporated herein.

Moreover, approval authority for the use of UAS will be set at an appropriate and consistent level across the Department. At a minimum, each time UAS are deployed, approval must be granted (1) at the Assistant Special Agent in Charge-or-equivalent level at the relevant field office, and (2) by an executive level supervisor within the agency's aviation support unit or a designated executive level supervisor at the agency's headquarters. Additionally, since the Department may only operationally deploy UAS in connection with authorized investigations or activities, supervisors must ensure that the underlying investigations themselves have been authorized consistent with applicable guidelines and other Department policies.

Finally, federal records must be captured, managed, and retained in a manner consistent with the Federal Records Act and all other applicable authorities. As with federal records collected by other investigative tools, components are obligated to retain UAS-collected data in accordance with applicable records retention schedules.

ONGOING POLICY MANAGEMENT

As UAS technology evolves and improves, it is important that the Department continue to have adequate information about its use to ensure strategic alignment and proper evaluation of the Department's policy. To that end, this policy imposes certain new requirements.

Each component that uses UAS must designate a point of contact through which field offices will report the information outlined below to the component's headquarters and Department leadership on the use of UAS on an ongoing basis.

In addition, Department agencies that use UAS must report annually to the Deputy Attorney General on the use of UAS. The report should incorporate privacy reviews, as well as the number of UAS operational deployments (not including training or research and development flights) conducted during the reporting period and a brief description of types or categories of missions flown along with the number of each type of mission. Additionally, to the extent the agency sought assistance from, or provided assistance to, another federal, state, local, or tribal agency during the relevant time period, the number of these operational deployments and a brief

description of types or categories of missions flown along with the number of each type of mission should also be provided.

Components that have not previously disclosed any UAS operations as part of these annual reporting requirements, or that have discontinued UAS use for the duration of an annual reporting period, must notify the Deputy Attorney General prior to initiating or re-introducing UAS operations.

Department leadership will continue to engage in meaningful review of UAS as the technology advances. To facilitate this review, a standing committee comprised of a broad range of Department components will meet twice a year to evaluate any policy or regulatory changes that may be needed as a result of innovations or developments in UAS technology.

TRANSPARENCY

Rigorous adherence to the requirements set forth in this policy is not enough—to be successful in our law enforcement and national security missions, we must continue to facilitate relationships of trust with the communities we serve. Enhancing our transparency about agency operations, including how we operate UAS, creates an informed citizenry and greater confidence in the Department's decision-making.

Education of the public can enhance the Department's ability to fulfill its missions and serve the American people. As appropriate, while not revealing information that might compromise law enforcement or national security needs, the Department will update its website to reflect its current policy on UAS on an ongoing basis, and will provide a general summary of UAS operations conducted by the Department during the previous year, including a brief description of types or categories of missions flown and the number of times the Department provided assistance to other federal, state, local and tribal agencies or entities.

APPENDIX 15

International Association of Chiefs of Police (IACP) sUAS Concepts and Issues Paper and Model Policy

IACP LAW ENFORCEMENT POLICY CENTER

Small Unmanned Aircraft Systems

Concepts and Issues Paper

May 2015

I. INTRODUCTION

A. Purpose of the Document

This paper is designed to accompany the *Model Policy on Small Unmanned Aircraft Systems* published by the IACP Law Enforcement Policy Center. This paper provides essential background material and supporting documentation to provide a greater understanding of the developmental philosophy and implementation requirements for the model policy for most state, local, and tribal public safety applications of sUAS technology. This material will be of value to law enforcement executives in their efforts to tailor the model to the requirements and circumstances of their communities and their law enforcement agencies.

B. Background

The use of aircraft in support of law enforcement operations has been an integral part of many agencies' public safety mission for years. The ability to provide an aerial view has been invaluable in search and rescue, tactical, emergency response, and investigative missions. However, because airborne assets, including helicopters and fixed wing aircraft, require extensive training, maintenance, and regulatory commitments, often only largeS agencies with sufficient resources can support airborne operations.

Recently, technological advances have allowed public safety agencies to consider the acquisition of small unmanned aircraft systems (sUAS) to support their operations. These devices are small, lightweight, remotely controlled aircraft that can be equipped with cameras or other sensors and quickly deployed. The sUAS can provide many of the advantages of traditional aircraft, but at a fraction of the cost. In some cases, these aircraft can be deployed in situations where manned aircraft are unavailable or conditions could be prohibitively dangerous to pilots and persons on the ground.

While government regulations are still in development, many public safety agencies may find sUAS to be a valuable addition to their operations. The advantages and special policy considerations of sUAS operations will be discussed further in this document.

The use of large unmanned aircraft by the military and some federal enforcement initiatives has been widely reported in the media. However, such systems are generally unsuited for the purpose and applications of state, local, and tribal public safety agencies. This paper, and the accompanying Model Policy, are limited to the discussion of small unmanned aircraft systems, defined by the Federal Aviation Administration (FAA) as 55 pounds or less.

C. Uses for sUAS

Agencies currently using sUAS have found them to be invaluable tools in a number of operational applications. Because of their size, many sUAS can be carried in the trunk of a patrol car and quickly deployed at an incident. In the case of an overturned tank truck, for instance, the sUAS can quickly deliver an aerial view of the scene, providing enhanced situational awareness and allowing responders to develop an effective response, while documenting the scene for subsequent investigation. In the case of a hazardous material spill, the sUAS might be deployed where it could be unsafe for human pilots or first responders. An sUAS could also be equipped with sensors to detect the presence of hazardous materials.

A publication of the IACP Law Enforcement Policy Center
44 Canal Center Plaza, Suite 200, Alexandria, VA 22314

This document is the result of work performed by the IACP Law Enforcement Policy Center. The views and opinions expressed in this document are sanctioned by the center's advisory board and do not necessarily represent the official position or policies of the International Association of Chiefs of Police.

Many agencies use an sUAS for photographing crime or accident scenes. Unlike a manned helicopter, a small, battery-operated multi-rotor unmanned aircraft can hover above a scene with minimal disturbance from the downward-forced air from the rotors. The aerial view provides a unique perspective than can be employed for computer modeling and subsequent reconstruction of a scene. Similarly, aerial imaging of schools, public facilities, or critical infrastructure within an agency's jurisdiction could be used in training or developing response plans in case of a future incident.

Search and rescue missions are often cited by agencies considering acquisition of an sUAS. In a recent case in Canada, a thermal imaging sensor on an sUAS was employed to find an injured driver who wandered away from an accident in a remote area.[1] An sUAS may be able to operate in terrain or conditions that are unsuitable for manned aircraft. They can be quickly deployed to monitor evacuation routes in a natural disaster or traffic around a special event. Some agencies have considered the use of an sUAS to provide an emergency communications link when other systems are down because of power outages or the loss of communication towers.

Because of their small size and relatively quiet operation, sUAS can also be useful in tactical situations, providing views of the scene to increase situational awareness and assist in planning a response to minimize risk to officers and the public. Video recordings from the aircraft can be valuable evidence in support of an investigation.

II. ADMINISTRATIVE AND REGULATORY RESTRICTIONS ON sUAS

The usefulness of sUAS has been clearly demonstrated; however, their utility is limited by FAA rules governing their use. The FAA is responsible for ensuring the safe operation of any aircraft within the National Airspace System (NAS). On February 14, 2012, Congress passed the *FAA Modernization and Reform Act of 2012* that included a provision requiring the FAA to "…develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system."[2] The legislation established a deadline of September 30, 2015, to complete the plan. This document will not attempt to address all FAA regulations, but will briefly discuss some of the relevant issues that an agency must consider before introducing an sUAS into agency operations.[3]

The very first step an agency should undertake is an assessment of agency operations and determination of how the sUAS will be employed to further the agency's mission. There are many types of sUAS available, and it is critical to identify the ways an agency will use the technology in order to identify the system that most closely meets the agency's operational needs. For instance, an agency that is frequently called upon for search and rescue missions in remote areas may consider a small, hand-launched, fixed wing aircraft with a long flight duration. Agencies looking for a quickly deployable aircraft to provide enhanced situational awareness in an emergency or documentation of a scene might find greater utility in a multi-rotor aircraft with a high degree of maneuverability but shorter flight duration. Some agencies have successfully employed several types of sUAS, deploying the most appropriate tool for the task at hand. Taking the time to review agency operations and identify the sUAS that will provide the greatest functionality can help ensure the success of an sUAS initiative.

All law enforcement entities are required to obtain a Certificate of Authorization (COA) from the FAA before undertaking any flight operations. The FAA Unmanned Aircraft Systems Integration Office (UASIO) has been established to assist agencies and organizations to navigate the COA process. It is recommended that an agency contact the UASIO early in the process to determine the requirements of a COA. Each agency's COA will be unique to the jurisdiction to which it will apply. The location of airports (including many small general aviation facilities), congested urban areas, and geography could all require special operating rules; for instance, in some cases multiple COAs may be required with stricter altitude restrictions within a certain proximity of an airfield than in other portions of the jurisdiction. A COA may require as many as three operators for sUAS operations, with a pilot who is required to maintain visual contact with the aircraft at all times, a spotter to look out for other aircraft, and a dedicated camera operator.

In addition to federal regulations, some states and local governments have introduced legislation that could impact law enforcement operation of the technology. It is important to fully understand all federal, state, and local laws governing the use of sUAS and the data collected through their use.

---

[1] John Weidlich, "Aerial Drone Locates Sask. Man Injured in Rollover Crash," CBC News, May 09, 2013, http://www.cbc.ca/news/canada/saskatchewan/aerial-drone-locates-sask-man-injured-in-rollover-crash-1.1398942 (accessed May 6, 2015).

[2] FAA Modernization and Reform Act of 2012, Pub. L 112–95 (February 14, 2012), http://www.gpo.gov/fdsys/pkg/PLAW-112publ95/pdf/PLAW-112publ95.pdf (accessed May 6, 2015).

[3] A full discussion of sUAS regulations for public safety and resources for establishing an sUAS program can be found on the FAA web site, http://www.faa.gov.

International Association of Chiefs of Police (IACP) sUAS Concepts and Issues Paper and Model Policy, continued

A. Privacy Concerns of sUAS Operations

The potential deployment of sUAS by law enforcement agencies has prompted concerns that their use could result in violations of privacy and civil liberties. Public attitudes toward law enforcement use of unmanned aircraft can vary widely from jurisdiction to jurisdiction. It is important for an agency to recognize these concerns and develop policies to help safeguard the privacy of the public they serve. The Model Policy provides guidance that specifically addresses privacy issues, but every community is unique, so public engagement is crucial to the success of the program; for these reasons, the range of issues and concerns are far too complex and varied to discuss in depth in this paper. The publications below will provide further discussion of the issues an agency must consider when introducing sUAS initiatives in their communities.

The IACP has developed a document, *IACP Technology Policy Framework*, to help agencies develop consistent policies across all technology platforms while considering the impact of the technology on the community. The *Framework* lists nine universal principals to provide guidance during the development of policies for "technologies that can, or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data were captured."[4]

When developing an sUAS policy, an agency should be transparent and fully inform the public of the agency's intended uses of the technology. This is especially true for policies governing the retention and use of recorded audio, video, photographs, or other data acquired through the use of sUAS. All data collected should be for official use only, and access to recorded material strictly monitored.

For further information, the *Police Chief* magazine article, *Unmanned Aircraft Systems: All the Boxes Checked, but Challenges Remain* is an overview of sUAS operations for law enforcement.[5] A thorough review of the legal and policy issues surrounding the public safety use of sUAS can be found in the Brookings Institution publication, *Drones and Aerial Surveillance, Considerations for Legislators*.[6]

B. Procedures for Using sUAS

sUAS should be operated only by trained and authorized personnel, including all crew members. All flights should be approved by the appropriate authority and should be for a legitimate public safety mission, training, or demonstration purposes as defined by policy. Proper training of all personnel in operation as well as policy is critical for the success of a program.

All flights should be documented, accounting for all flight time of the sUAS. A reporting protocol specifically designed for sUAS operations should be developed and followed. An authorized supervisor should routinely audit all flight documentation, and any unauthorized use of the SUAS should result in strict accountability.

Except in instances when the safety of officers, the public, or an investigation could be compromised, agencies deploying sUAS in populated areas should consider informing the public, possibly employing Reverse 9-1-1, social media, email alerts, or even patrol car public address systems. This will provide a level of safety should the aircraft make an uncontrolled landing while helping to minimize public concern over the presence of the aircraft.

C. Record Control and Management

Reference has been made previously to the need for control and management of sUAS recordings to ensure the integrity of the recordings, secure the chain of custody where information of evidentiary value is obtained, and use recordings to their fullest advantage for training and other purposes. In order to accomplish these ends, officers and their supervisors should refer to their policies on records control, retention, and management.

D. Technical Capabilities

The use of sUAS by law enforcement is still in its infancy. Technology has brought considerable enhancements to law enforcement's capabilities. It has also introduced significant complexities. The use of such emerging technology by law enforcement has brought new concerns into aspects of search and seizure, privacy rights, and government data collection. Any agency currently using or considering the introduction of sUAS into its toolbox should remain cognizant of emerging case law. It is very likely the courts will be adding clarity to this complex issue in the near future.

---

[4] *IACP Technology Policy Framework* (Alexandria, VA: 2014), 3, http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf (accessed May 6, 2015).

[5] Brett Davis and Don Roby, "Unmanned Aircraft Systems: All the Boxes Checked, but Challenges Remain," *The Police Chief* 80 (June 2013): 60–63, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=2957&issue_id=62013 (accessed May 6, 2015).

[6] Gregory McNeal, *Drones and Aerial Surveillance: Considerations For Legislators* (Washington, D.C.: The Brookings Institution, Center for Technology Innovation, November 2014), http://www.brookings.edu/research/reports2/2014/11/drones-and-aerial-surveillance (accessed May 6, 2015).

E. References

Information regarding technical capabilities and advancement in sUAS can be found through the following:

- Airborne Law Enforcement Association
  www.alea.org
- Association for Unmanned Vehicle Systems International
  www.auvsi.org
- Federal Aviation Administration
  www.faa.gov

Acknowledgment

This document was developed by the IACP Law Enforcement Policy Center in cooperation with the IACP Aviation Committee.

Every effort has been made by the IACP Law Enforcement Policy Center staff and advisory board to ensure that this document incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

IACP Law Enforcement Policy Center Staff: Philip Lynn, Manager; Sara Dziejma, Project Specialist; and Vincent Talucci, Executive Director, International Association of Chiefs of Police.

© Copyright 2015. International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. No reproduction of any part of this material may be made without prior written consent of the copyright holder.

International Association of Chiefs of Police (IACP) sUAS Concepts and Issues Paper and Model Policy, continued

SMALL UNMANNED AIRCRAFT SYSTEMS

Model Policy

Effective Date May 2015		*Number*
Subject Small Unmanned Aircraft Systems		
Reference		*Special Instructions*
Distribution	*Reevaluation Date*	*No. Pages* 3

I. PURPOSE

This policy is intended to provide personnel who are assigned responsibilities associated with the deployment and use of small unmanned aircraft systems (sUAS) with instructions on when and how this technology and the information it provides may be used for law enforcement and public safety purposes in accordance with law.[1]

II. POLICY

It is the policy of this department that duly trained and authorized agency personnel may deploy sUAS when such use is appropriate in the performance of their official duties, and where deployment and use, and the collection and use of any audio/video recordings or other data originating from or generated by the sUAS, comport with the policy provisions provided herein and applicable law.

III. DEFINITIONS

Digital Multimedia Evidence (DME): Digital recording of images, sounds, and associated data.

Model Aircraft: A remote controlled aircraft used by hobbyists that is built, produced, manufactured, and operated for the purposes of sport, recreation, and/or competition.

Unmanned Aircraft (UA) or Unmanned Aerial Vehicle (UAV): An aircraft that is intended to navigate in the air without an on-board pilot. Also alternatively called Remotely Piloted Aircraft (RPA), Remotely Operated Vehicle (ROV), or Drone.

Unmanned Aircraft System (UAS): A system that includes the necessary equipment, network, and personnel to control an unmanned aircraft.

Small Unmanned Aircraft Systems (sUAS): UAS systems that utilize UAVs weighing less than 55 pounds and are consistent with Federal Aviation Administration (FAA) regulations governing model aircraft.

UAS Flight Crewmember: A pilot, visual observer, payload operator or other person assigned duties for a UAS for the purpose of flight or training exercise.

Unmanned Aircraft Pilot: A person exercising control over a UA/UAV/UAS during flight.

IV. PROCEDURES

A. Administration

All deployments of sUAS must be specifically authorized by the chief executive officer (CEO) of this agency or authorized supervisory personnel. This agency has adopted the use of sUAS to provide an aerial visual perspective in responding to emergency situations and exigent circumstances, and for the following objectives:

1. Situational Awareness: To assist decision makers (e.g., incident command staff; first responders; city, county, and state officials) in understanding the nature, scale, and scope of an incident—and for planning and coordinating an effective response.
2. Search and Rescue: To assist missing person investigations, AMBER Alerts, Silver Alerts, and other search and rescue missions.

[1] Some states have statutes that govern operation of UAS by public safety agencies. Consult your legal counsel for state and local laws that affect your agency.

1

3. Tactical Deployment: To support the tactical deployment of officers and equipment in emergency situations (e.g., incidents involving hostages and barricades, support for large-scale tactical operations, and other temporary perimeter security situations).
4. Visual Perspective: To provide an aerial visual perspective to assist officers in providing direction for crowd control, traffic incident management, special circumstances, and temporary perimeter security.
5. Scene Documentation: To document a crime scene, accident scene, or other major incident scene (e.g., disaster management, incident response, large-scale forensic scene investigation).

B. Procedures for sUAS Use
1. The agency must obtain applicable authorizations, permits, or certificates required by the Federal Aviation Administration (FAA) prior to deploying or operating the sUAS, and these authorizations, permits, and certificates shall be maintained and current.
2. The sUAS will be operated only by personnel (pilots and crew members) who have been trained and certified in the operation of the system.
3. The sUAS-certified personnel shall inspect and test sUAS equipment prior to each deployment to verify the proper functioning of all equipment and the airworthiness of the device.
4. The sUAS equipment is the responsibility of individual officers and will be used with reasonable care to ensure proper functioning. Equipment malfunctions shall be brought to the attention of the officer's supervisor as soon as possible so that an appropriate repair can be made or a replacement unit can be procured.
5. The sUAS equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the agency.
6. All flights will be documented on a form or database designed for that purpose, and all flight time shall be accurately recorded. In addition, each deployment of the sUAS shall include information regarding the reason for the flight; the time, date, and location of the flight; the name of the supervisor approving the deployment and the staff assigned; and a summary of the activities covered, actions taken, and outcomes from the deployment.
7. Except for those instances where officer safety or investigation could be jeopardized—and where reasonably possible and practical, agencies should consider notifying the public.
8. Where there are specific and articulable grounds to believe that the sUAS will collect evidence of criminal wrongdoing and/or if the sUAS will be used in a manner that may intrude upon reasonable expectations of privacy, the agency will obtain a search warrant prior to conducting the flight.

C. Restrictions on Using the sUAS
1. The sUAS shall be deployed and used only to support official law enforcement and public safety missions.
2. The sUAS shall not be operated in an unsafe manner or in violation of FAA rules.
3. The sUAS shall not be equipped with weapons of any kind.

D. DME Retention and Management
1. All DME shall be handled in accordance with existing policy on data and record retention, where applicable.
2. All DME shall be securely downloaded at the completion of each mission. The sUAS-certified operators will record information for each file that shall include the date, time, location, and case reference numbers or other mission identifiers—and identify the sUAS personnel involved in mission.
3. Officers shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute in any manner sUAS DME without prior written authorization and approval of the CEO or his or her designee.
4. All access to sUAS DME must be specifically authorized by the CEO or his or her designee, and all access is to be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes.
5. Files should be securely stored in accordance with agency policy and state records retention laws and retained no longer than necessary for purposes of training or for use in an investigation or prosecution.

E. sUAS Supervision and Reporting
1. sUAS supervisory personnel shall manage all deployments and uses of sUAS to ensure that officers equipped with sUAS devices utilize them in accordance with policy and procedures defined herein.

International Association of Chiefs of Police (IACP) sUAS Concepts and Issues Paper and Model Policy, continued

2. An authorized sUAS supervisor or 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.
3. The CEO of the agency or his or her designee shall publish an annual report documenting the agency's deployment and use of sUAS devices.

F. Training

1. Police personnel who are assigned sUAS must complete an agency-approved training program to ensure proper use and operations. Additional training may be required at periodic intervals to ensure the continued effective use and operation and proper calibration and performance of the equipment and to incorporate changes, updates, or other revisions in policy and equipment.
2. All agency personnel with sUAS responsibilities, including command officers, shall also be trained in the local and federal laws and regulations, as well as policies and procedures governing the deployment and use of sUAS.

Acknowledgment

This document was developed by the IACP Law Enforcement Policy Center in cooperation with the IACP Aviation Committee.

Every effort has been made by the IACP Law Enforcement Policy Center staff and advisory board to ensure that this document incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

IACP Law Enforcement Policy Center Staff: Philip Lynn, Manager; Sara Dziejma, Project Specialist; and Vincent Talucci, Executive Director, International Association of Chiefs of Police.

© Copyright 2015. Departments are encouraged to use this policy to establish one customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.

APPENDIX 16

International Association of Chiefs of Police (IACP) Technology Policy Framework

IACP TECHNOLOGY POLICY FRAMEWORK[1]
January 2014

Introduction
New and emerging technologies increasingly play a crucial role in the daily work of police, equipping officers with enforcement and investigative tools that have the potential of making them safer, better informed, and more effective and efficient. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

Technological advances have made it possible to monitor and record nearly every interaction between police and the public through the use of in-car and body-worn video, access to an expanding network of public and private video surveillance systems, and the increasing use of smartphones with digital recording capabilities by citizens and officers alike. Police can track suspects with the use of GPS tracking technologies and officers themselves can be tracked with automated vehicle location (AVL) systems. Automated license plate recognition (ALPR) systems can scan the license plates of vehicles within sight of officers in the field and quickly alert them if the vehicle has been reported stolen or is wanted. Identity can be remotely verified or established with biometric precision using mobile fingerprint scanners and facial recognition software. Crimes can be mapped as they are reported, gunshot detection technology can alert law enforcement almost instantaneously when a firearm is discharged, and surveillance cameras can be programmed to focus in on the gunshot location and stream live video to both dispatchers and responding officers. With these advancements come new opportunities to enhance public and officer safety. They also present new challenges for law enforcement executives.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology *can* be implemented, does not mean that it *should* be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

International Association of Chiefs of Police (IACP) Technology Policy Framework, continued

Addressing these challenges is paramount because of the broader issues that the use of this expanding array of technologies by law enforcement presents. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe.

The Policy Mandate

Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and to maintain community trust. Policies function to reinforce training and to establish an operational baseline to guide officers and other personnel in proper procedures regarding its use. Moreover, policies help to ensure uniformity in practice across the agency and to enforce accountability. Policies should reflect the mission and values of the agency and be tightly aligned with applicable local, state, and federal laws, regulations, and judicial rulings.

Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance. The use of automated license plate recognition (ALPR) technologies, unmanned aerial systems, and body-worn video by law enforcement, for example, has generated substantial public discussion, increasing scrutiny, and legislative action in recent years.[2] Privacy advocates, elected officials, and members of the public have raised important questions about how and under what circumstances these technologies are deployed, for what purposes, and how the data gathered by these technologies are retained, used, and shared. Having and enforcing a strong policy framework enables law enforcement executives to demonstrate responsible planning, implementation, and management.

Agencies should adopt and enforce a technology policy framework that addresses technology objectives, deployment, privacy protections, records management, data quality, systems security, data retention and purging, access and use of stored data, information sharing, accountability, training, and sanctions for non-compliance. Agencies should implement safeguards to ensure that technologies will not be deployed in a manner that could violate civil rights (race, religion, national origin, ethnicity, etc.) or civil liberties (speech, assembly, religious exercise, etc.). The policy framework is but one of several critical components in the larger technology planning effort that agencies should undertake to ensure proper and effective use of automation.

Universal Principles

Given the privacy concerns and sensitivity of personally identifiable information and other data often captured and used by law enforcement agencies,[3] and recognizing evolving perceptions of what constitutes a reasonable expectation of privacy,[4] the

technology policy framework should be anchored in principles universally recognized as essential in a democratic society.

The following universal principles should be viewed as a guide in the development of effective policies for *technologies that can, or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data were captured*.[5]

1. *Specification of Use*—Agencies should define the purpose, objectives, and requirements for implementing specific technologies, and identify the types of data captured, stored, generated, or otherwise produced.
2. *Policies and Procedures*—Agencies should articulate in writing, educate personnel regarding, and enforce agency policies and procedures governing adoption, deployment, use, and access to the technology and the data it provides. These policies and procedures should be reviewed and updated on a regular basis, and whenever the technology or its use, or use of the data it provides significantly changes.
3. *Privacy and Data Quality*—The agency should assess the privacy risks and recognize the privacy interests of all persons, articulate privacy protections in agency policies, and regularly review and evaluate technology deployment, access, use, data sharing, and privacy policies to ensure data quality (i.e., accurate, timely, and complete information) and compliance with local, state, and federal laws, constitutional mandates, policies, and practice.
4. *Data Minimization and Limitation*—The agency should recognize that only those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be deployed, and only for so long as it demonstrates continuing value and alignment with applicable constitutional, legislative, regulatory, judicial, and policy mandates.
5. *Performance Evaluation*—Agencies should regularly monitor and evaluate the performance and value of technologies to determine whether continued deployment and use is warranted on operational, tactical, and technical grounds.
6. *Transparency and Notice*—Agencies should employ open and public communication and decision-making regarding the adoption, deployment, use, and access to technology, the data it provides, and the policies governing its use. When and where appropriate, the decision-making process should also involve governing/oversight bodies, particularly in the procurement process. Agencies should provide notice, when applicable, regarding the deployment and use of technologies, as well as make their privacy policies available to the public. There are practical and legal exceptions to this principle for technologies that are

International Association of Chiefs of Police (IACP) Technology Policy Framework, continued

lawfully deployed in undercover investigations and legitimate, approved covert operations.[6]

7. *Security*—Agencies should develop and implement technical, operational, and policy tools and resources to establish and ensure appropriate security of the technology (including networks and infrastructure) and the data it provides to safeguard against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle includes meeting state and federal security mandates (e.g., the FBI's CJIS Security Policy[7]), and having procedures in place to respond if a data breach, loss, compromise, or unauthorized disclosure occurs, including whether, how, and when affected persons will be notified, and remedial and corrective actions to be taken.[8]
8. *Data Retention, Access and Use*—Agencies should have a policy that clearly articulates that data collection, retention, access, and use practices are aligned with their strategic and tactical objectives, and that data are retained in conformance with local, state, and/or federal statute/law or retention policies, and only as long as it has a demonstrable, practical value.
9. *Auditing and Accountability*—Agencies and their sworn and civilian employees, contractors, subcontractors, and volunteers should be held accountable for complying with agency, state, and federal policies surrounding the deployment and use of the technology and the data it provides. All access to data derived and/or generated from the use of relevant technologies should be subject to specific authorization and strictly and regularly audited to ensure policy compliance and data integrity. Sanctions for non-compliance should be defined and enforced.

Developing Policies and Operating Procedures

The universal principles provide structural guidance for the development of specific agency policies and operating procedures that comport with established constitutional, legal, and ethical mandates and standards. Agency policies and procedures specify the operational components of each individual technology implementation, deployment, and management, and should typically include and address the following factors:[9]

1. Purpose
    a. A general discussion of the purpose of a specific agency policy to include the agency's position on protecting privacy.
2. Policy
    a. A discussion of the overarching agency policy regarding the deployment and use of a specific technology, its application to members of the agency, and reference to relevant laws, policies, and/or regulations that authorize the agency to implement a technology, or that relate to the use and deployment of a technology.
3. Definitions

a. A description of the technology, its components, and functions.
b. Definitions and acronyms associated with the technology.

4. Management
   a. Strategic Alignment: Describe how the technology aligns and furthers the agency's strategic and tactical deployment objectives.
   b. Objectives and Performance: Identify objectives for the deployment and conditions for use of a technology, and a general strategy for assessing performance and compliance with the agency's policy.
   c. Ownership: Clearly specify that the hardware and software associated with the technology is the property of the agency, regardless whether it has been purchased, leased, or acquired as a service, and that all deployments of a technology are for official use only (FOUO). All data captured, stored, generated, or otherwise produced by a technology are the property of the agency, regardless where the data are housed or stored. All access, use, sharing, and dissemination of the data must comply with the policies established and enforced by the agency.
   d. Classification of Data: Clearly specify the data classification and its level of sensitivity (e.g., top secret, secret, confidential, restricted, unclassified, private, public, etc.), whether the data captured, stored, generated, or otherwise produced by a technology are considered public information, and whether it is subject to applicable public records act requests and under what circumstances.
   e. Privacy Impact: Develop or adopt and use a formal privacy impact assessment (PIA)[10] or similar agency privacy assessment on technology and the data it captures, stores, generates, or otherwise produces.

5. Operations
   a. Installation, Maintenance, and Support: Require regular maintenance, support, upgrades, calibration, and refreshes of a technology to ensure that it functions properly.
   b. Deployment: Identify who is authorized to officially approve the deployment and use of a technology, and the conditions necessary for deployment and use, if applicable.
   c. Training: Require training, and perhaps certification or other documented proficiency, if applicable, of all personnel who will be managing, maintaining, and/or using a technology. Training should also cover privacy protections on the use of the technology, and the impact and sanctions for potential violations.
   d. Operational Use: Identify specific operational factors that must be addressed in deployment and use of a technology. (For example, for ALPR, the officer should i) verify that the system has correctly "read" the license plate characters; ii) verify the state of issue of the license plate; iii) verify that the "hot list" record that triggered the alert is still active in the state or NCIC stolen vehicle or other file, and confirm the

International Association of Chiefs of Police (IACP) Technology Policy Framework, continued

hit with the entering agency; and iv) recognize that the driver of the vehicle may not be the registered owner).

e. Recordkeeping: Require recordkeeping practices that document all deployments of the technology, including who authorized the deployment; how, when, and where the technology was deployed; results of deployments; and any exceptions. Recordkeeping will support efforts to properly manage technology implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help document business benefits realization.

6. Data Collection, Access, Use, and Retention
   a. Collection: Define what data will be collected, how data will be collected, the frequency of collection, how and where data will be stored, and under what authority and conditions the data may be purged, destroyed, or deleted in compliance with applicable local, state, and/or federal recordkeeping statutes and policies, court orders, etc. Identify the destruction/deletion methods to be used.
   b. Access and Use: Define what constitutes authorized use of data captured, stored, generated, or otherwise produced by a technology. Define who is authorized to approve access and use of the data, for what purposes and under what circumstances.
   c. Information Sharing: Specify whether data captured, stored, generated, or otherwise produced by a technology can be shared with other agencies, under what circumstances, how authorization is provided, how information that is shared is tracked/logged, how use is monitored, and how policy provisions (including privacy) will be managed and enforced. Any agency contributing and/or accessing shared information should be a signatory of a data sharing Memorandum of Understanding (MOU). Dissemination of any shared information should be governed by compliance with applicable state and federal laws, standards, agency privacy policies, and procedures as agreed in the MOU.
   d. Security: Define information systems security requirements of the technology and access to the data to ensure the integrity of the systems and confidentiality of the data. The security policy should address all state and federal mandated security policies, and clearly address procedures to be followed in the event of a loss, compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data, including how and when affected persons will be notified, and remedial and corrective actions to be taken.
   e. Data Retention and Use: Establish data retention schedules in accordance with state or federal law or policy, access privileges, purge,

and deletion criteria for all data captured, stored, generated, or otherwise produced by a technology. Agencies should consider differentiating between data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion or direct investigative focus. Agencies may wish to limit the retention of general surveillance data. Empirical research assessing the performance of a technology may assist in determining an appropriate retention schedule.

7. Oversight, Evaluation, Auditing, and Enforcement
    a. Oversight: Establish a reporting mechanism and a protocol to regularly monitor the use and deployment of a technology to ensure strategic alignment and assessment of policy compliance.
    b. Evaluation: Regularly assess the overall performance of a technology so that it can i) identify whether a technology is performing effectively, ii) identify operational factors that may impact performance effectiveness and/or efficiency, iii) identify data quality issues, iv) assess the business value and calculate return on investment of a technology, and v) ensure proper technology refresh planning.
    c. Auditing: Audit all access to data captured, stored, generated, or otherwise produced by a technology to ensure that only authorized users are accessing the data for legitimate and authorized purposes, and establish regular audit schedules.
    d. Enforcement: Establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with agency policies.

Conclusion

Realizing the value that technology promises law enforcement can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all resources and tools available to law enforcement, the use of new technologies must be carefully considered and managed. Agencies must clearly articulate their strategic goals for the technology, and this should be aligned with the broader strategic plans of the agency and safety needs of the public. Thorough and ongoing training is required to ensure that the technology performs effectively, and that users are well versed in the operational policies and procedures defined and enforced by the agency. Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system, and reassure the public that their privacy interests are recognized and protected. The development of these policies is a proven way for executives to ensure they are taking full advantage of technology to assist in providing the best criminal justice services, while protecting the privacy, civil rights, and civil liberties of citizens.

International Association of Chiefs of Police (IACP) Technology Policy Framework, continued

[1] This Technology Policy Framework was developed by an ad-hoc committee of law enforcement executives and subject matter experts representing IACP Divisions, Committees, Sections, the IACP National Law Enforcement Policy Center, and other organizations and groups, including the Criminal Intelligence Coordinating Council, Major Cities Chiefs Association, National Sheriffs' Association, Major County Sheriffs' Association, Association of State Criminal Investigative Agencies, the Institute for Intergovernmental Research (IIR), the Integrated Justice Information Systems (IJIS) Institute, and federal partners.

[2] The American Civil Liberties Union (ACLU) recently released two reports addressing law enforcement technologies—ALPR and body-worn video. Both reports discuss the value of the technology to law enforcement operations and investigations, and both call for policies addressing deployment, operations, data retention, access, and sharing. Catherine Crump, *You are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements,* (New York: ACLU, July 2013), at https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record, and Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All,* (New York: ACLU, October 2013), at https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all. *Also see,* Massachusetts Senate Bill S.1648, *An Act to Regulate the Use of Automatic License Plate Reader Systems,* Cynthia S. Creem, Sponsor, at https://malegislature.gov/Bills/188/Senate/S1648; Cynthia Stone Creem and Jonathan Hecht, "Check it, then chuck it," *The Boston Globe,* December 20, 2013, at http://www.bostonglobe.com/opinion/2013/12/20/podium-license/R1tKQerV0YAPLW6VCKodGK/story.html; Shawn Musgrave, "Boston Police halt license scanning program," *The Boston Globe,* December 14, 2013, at http://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-licence-plate-readers-amid-privacy-concerns/B2hy9UIzC7KzebnGyQ0JNM/story.html; Ashley Luthern and Kevin Crowe, "Proposed Wisconsin bill would set rules for license-plate readers," *Milwaukee Journal Sentinel*, December 3, 2013, at http://www.jsonline.com/news/milwaukee/proposed-wisconsin-bill-would-set-rules-for-license-plate-readers-b99155494z1-234324371.html; Dash Coleman, "Tybee Island abandons license plate scanner plans," *Savannah Morning News,* December 3, 2013, at http://savannahnow.com/news/2013-12-02/tybee-island-abandons-license-plate-scanner-plans#.UqCAy8RDuN0; Kristian Foden-Vencil, "Portland police are collecting thousands of license plate numbers every day," *Portland Tribune*, December 3, 2013, at http://portlandtribune.com/pt/9-news/203130-portland-police-are-collecting-thousands-of-license-plate-numbers-every-day; Alicia Petska, "City Council split over how to handle license plate reader concerns," *The News & Advance,* (Lynchburg, VA), November 12, 2013, at http://www.newsadvance.com/news/local/article_5327dc78-4c18-11e3-bc28-001a4bcf6878.html; Jonathan Oosting, "Proposal would regulate license plate readers in Michigan, limit data stored by police agencies," *MLive,* (Lansing, MI), September 9, 2013, at http://www.mlive.com/politics/index.ssf/2013/09/proposal_would_regulate_licens.html; Katrina Lamansky, "Iowa City moves to ban traffic cameras, drones, and license plate recognition," *WQAD*, June 5, 2013, at http://wqad.com/2013/06/05/iowa-city-moves-to-ban-traffic-cameras-drones-and-license-plate-recognition/; Richard M. Thompson, II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses,* (Washington, DC: Congressional Research Service, April 3, 2013), at http://www.fas.org/sgp/crs/natsec/R42701.pdf; Somini Sengupta, "Rise of Drones in U.S. Drives

Efforts to Limit Police Use," *New York Times,* February 15, 2013, at http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?pagewanted=all; Stephanie K. Pell and Christopher Soghoian, "Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact," *Berkeley Technology Law Journal,* Vol. 27, No. 1, pp. 117-196, (2012), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644; and Stephen Rushin, "The Legislative Response to Mass Police Surveillance," 79 *Brooklyn Law Review* 1*,* (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344805. All accessed December 30, 2013.

[3] Personally identifiable information (PII) has been defined as "…any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Government Accountability Office (GAO), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (Washington, D.C.: GAO, May 2008), p. 1, at http://www.gao.gov/new.items/d08536.pdf. McCallister, *et. al.,* define "linked" information as "information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual." Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* (Gaithersburg, MD: NIST, April 2010), p. 2-1, at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. McCallister, *et. al.,* go on to describe *linked* and *linkable* information: "For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable." *Id.* Both accessed December 30, 2013.

[4] Justice Harlan first articulated a "constitutionally protected reasonable expectation of privacy" in *Katz v. United States*, 389 U.S. 347 (1967), at 361. Justice Harlan's two-fold test is "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* Many of the technologies being deployed by law enforcement capture information that is publicly exposed, such as digital photographs and video of people and vehicles, or vehicle license plates in public venues (i.e., on public streets, roadways, highways, and public parking lots), and there is little expectation of privacy. "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *United States v. Knotts*, 460 U.S. 276 (1983), at 281. Law enforcement is free to observe and even record information regarding a person's or a vehicle's movements in public venues. The U.S. Supreme Court, however, has ruled that the electronic compilation of otherwise publicly available but

International Association of Chiefs of Police (IACP) Technology Policy Framework, continued

difficult to obtain records alters the privacy interest implicated by disclosure of that compilation. *U.S. Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989). Automation overwhelms what the Court referred to as the *practical obscurity* associated with manually collecting and concatenating the individual public records associated with a particular person into a comprehensive, longitudinal criminal history record. "…[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.,* at p. 764. This has subsequently been referred to as the "mosaic theory" of the Fourth Amendment. *United States v. Maynard,* 615 F.3d 544 (D.C. Cir.) (2010). *See also,* Orin Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review*, Vol. 111, p. 311, (2012), at http://www.michiganlawreview.org/assets/pdfs/111/3/Kerr.pdf. Accessed December 30, 2013.

[5] These universal principles largely align with the Fair Information Practices (FIPs) first articulated in 1973 by the Department of Health, Education & Welfare (HEW). HEW, *Records, Computers and the Rights of Citizens*, July 1973, at http://epic.org/privacy/hew1973report/default.html. *See,* Robert Gellman, *Fair Information Practices: A Basic History,* Version 2.02, November 11, 2013, at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. Comparable principles have been articulated by various governmental agencies, including the U.S. Department of Homeland Security, (Hugo Teufel, III, *Privacy Policy Guidance Memorandum, Number: 2008-01,* (Washington, DC: DHS, December 29, 2008), pp. 3-4, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf); the Home Office in the United Kingdom (Home Office, *Surveillance Camera Code of Practice,* (London, UK; The Stationery Office, June 2013), pp 10-11, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf); and the Information and Privacy Commissioner of Ontario, Canada (Ann Cavoukian, *Guidelines for the Use of Video Surveillance Cameras in Public Places,* (Ontario, Canada: Information and Privacy Commissioner of Ontario, September 2007), pp. 5-6, at: http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf, and Ann Cavoukian, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigative Report (Privacy Investigation Report MC07-68)*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, March 3, 2008), p 3, at: http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf). *Also see*, National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment,* (The National Academies Press: Washington, D.C., 2008), at http://nap.edu/catalog.php?record_id=12452. All accessed December 30, 2013.

[6] Law enforcement is not, for example, expected to notify the subjects of lawfully authorized wiretaps that their conversations are being monitored and/or recorded. These deployments, however, are typically subject to prior judicial review and authorization. *See, e.g., Katz v. United States,* 389 U.S. 347 (1967); *Berger v. New York,* 388 U.S. 41 (1967); *Title III, Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2510-2522, as amended by the *Electronic Communications Privacy Act of 1986*.

[7] Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy,* Version 5.2, August 9, 2013, CJISD-ITS-DOC-08140-5.2, at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view. Accessed December 30, 2013.

[8] Additional guidance regarding safeguarding personally identifiable information can be found in the Office of Management and Budget (OMB) Data Breach notification policy (M-07-16), at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf, and state data breach notification laws available from the National Conference of State Legislatures, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Accessed December 30, 2013.

[9] *See, e.g.,* International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2010 http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223; Paula T. Dow, Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data,* (Trenton, NJ: Office of the Attorney General, December 3, 2010), at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf; Office of the Police Ombudsman, *2011 Annual Report: Attachment G: Body-Worn Video & Law Enforcement: An Overview of the Common Concerns Associated with Its Use*, (Spokane, WA: Spokane Police Ombudsman, February 20, 2012), at http://www.spdombudsman.com/wp-content/uploads/2012/02/Attachment-G-Body-Camera-Report.pdf; ACLU, *Model Policy: Mobile License Plate Reader (LPR) System,* (Des Moines, IA: ACLU, September 19, 2012), at http://www.aclu-ia.org/iowa/wp-content/uploads/2012/09/Model-ALPR-Policy-for-Iowa-Law-Enforcement.pdf. Many of these policy elements are also addressed in the National Research Council's report, *op. cit.,* specifically in chapter 2, "A Framework for Evaluating Information-Based Programs to Fight Terrorism or Serve Other Important National Goals," at pp. 44-67. All accessed December 30, 2013

[10] A privacy impact assessment (PIA) is "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme." Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review,* 25, 2 (April 2009), pp. 125-135, at http://www.rogerclarke.com/DV/PIAHist-08.html. Law enforcement agencies should consider using the Global Advisory Committee's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* at https://it.ojp.gov/gist/47/Guide-to-Conducting-Privacy-Impact-Assessments-for-State--Local--and-Tribal-Justice-Entities. This resource leads policy developers through appropriate privacy risk assessment questions that evaluate the process through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application. The IACP published *Privacy Impact Assessment Report for the Utilization of License Plate Readers,* (Alexandria, VA: IACP, September 2009), at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. For a list of PIAs completed by the U.S. Department of Justice, *see* http://www.justice.gov/opcl/pia.htm; Department of Homeland Security, *see* https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia. All accessed December 30, 2013.

Glossary

Certificate of Authorization (COA) – The documentation required by the FAA for a public entity to use an unmanned aircraft system.

Community policing – A philosophy that promotes organizational strategies that support the systemic use of partnerships and problem-solving techniques to proactively address the immediate conditions that give rise to public safety issues such as crime.

Drone - A popular term applied to unmanned aircraft systems. It has become primarily associated with military aircraft like the Predator.

Federal Aviation Administration (FAA) – A unit of the U.S. Department of Transportation, the FAA is charged with regulating and controlling all commercial flights in U.S. airspace. Under a congressional mandate, the agency must develop regulations integrating commercial and public unmanned aircraft system operations into the general airspace.

Gimbal system – A gimbal is a pivoted support that allows the rotation of an object about a single axis. A gimbal is often used in systems to allow for stabilization and balanced movement.

Global Positioning System (GPS) – A satellite navigation system used to determine the ground position of an object. A GPS system on a UAS allows the aircraft to remain in a stable position during operation, or can provide the basis for flying a set pattern without being controlled by a pilot.

Payload – The load carried by a vehicle or an aircraft system exclusive of what is necessary for its operation. In the case of unmanned aircraft systems, a payload most often includes still and video cameras, a global positioning system, an infrared camera and other sensors. Private operators have used UAS to carry payloads of merchandise and communications devices.

Privacy Impact Assessment (PIA) – A decision-making tool used to identify and mitigate privacy risks at the beginning and throughout the development life cycle of a program or system. It helps the public understand what information is being collected, and how it will be used, shared, accessed and stored.

Reasonable Expectation of Privacy (RXP) – A legal standard of the circumstances under which a person can claim the right to privacy. Courts have determined that a person can claim a reasonable expectation of privacy in their own home, but not in a public place like a park or city street. The concept of RXP fundamentally changed privacy law, but technological advances have called the RXP analysis into question. Court precedents have recently declared that police violate a person's RXP if they open files on a cellular phone or place a GPS on a vehicle without a warrant.

small Unmanned Aircraft System (sUAS) – A small version of a UAS, weighing less than 55 pounds. While Public Law 112-95 does not specify whether the 55-pound weight limit refers to the total weight of the aircraft with or without payload on board, the FAA has proposed a rule in which the 55-pound weight limit would include everything that is on board the aircraft.

Unmanned Aircraft Vehicle (UAV) – A powered aircraft that does not have onboard pilots (as defined by the DoD). The FAA uses the term Unmanned Aircraft (UA) instead of UAV.

Unmanned Aircraft System (UAS) – The aircraft and all of the associated support equipment, control station, data links, telemetry, communications, and navigation equipment necessary to operate it (as defined by the FAA).

References

A.B. 203, 2013-2014 Legis. Assem. (Wis. 2014).

A.B. 239, 78th Legis. Assem. (Nev. 2015).

Aircraft Owners and Pilots Association. 2015. "Pilot certificate options and timeline frequently asked questions." Accessed April 16, 2015. http://www.aopa.org/letsgoflying/ready/time/options.html.

Altigator. 2015. "Drone: OnyxStar Hydra-12 with 12Kg of payload – heavy lifting" [video file]. Accessed February 17, 2016. https://www.youtube.com/watch?v=tMPl6dI1ntA.

Amazon.com, Inc. 2015. "Amazon Prime Air Frequently Asked Questions." Accessed April 8, 2015. http://www.amazon.com/b?node=8037720011.

Appleby, J. 2013. "Small unmanned aircraft systems (sUAS) test and evaluation: Robotic aircraft for public safety (RAPS)." Lecture presented at the Small Unmanned Systems Business Exposition, San Francisco, July 26. http://www.slideshare.net/sUASNews/8-raps-26july13.

AP (Associated Press). 2012. *The AP-National Constitution Center Poll – August, 2012*. N.p.: Associated Press. http://surveys.ap.org/data/GfK/AP-NCC%20Poll%20August%20GfK%202012%20Topline%20FINAL_PRIVACY.pdf.

Appropriations Act of 2013, S.B. 402 section 7.16(e), 2013 Gen. Assem. (N.C. 2013).

Arlington Police Department. 2015. "Frequently Asked Questions About the Aviation Unit." Accessed February 4, 2015. http://www.arlington-tx.gov/police/aviation-unit/.

AUVSI (Association for Unmanned Vehicle Systems International). 2013. *The Economic Impact of Unmanned Aircraft Systems Integration in the United States*. Arlington, Virgina: AUVSI. http://www.auvsi.org/auvsiresources/economicreport.

———. 2015. *Snapshot of the First 500 Commercial UAS Exemptions*. Arlington, Virgina: AUVSI. http://higherlogicdownload.s3.amazonaws.com/AUVSI/f28f661a-e248-4687-b21d-34342433abdb/UploadedFiles/Section333Report.pdf.

———. 2016. *Code of Conduct*. Accessed February 2, 2016. http://www.auvsi.org/conduct

BBC News. 2014. "Drone operator explains how he found missing man." *BBC News – Technology*, July 25. http://www.bbc.com/news/technology-28423252.

Beary, Richard. 2015. Testimony in *Hearing Before House Comm. on Homeland Security Subcomm. on Oversight and Management Efficiency*, 114th Cong. 9. http://docs.house.gov/meetings/HM/HM09/20150318/103136/HHRG-114-HM09-Wstate-BearyR-20150318.pdf.

Bittel, J. 2013. "German pirate party uses drone to crash Angela Merkel event." *Slate*, September 18. http://www.slate.com/blogs/future_tense/2013/09/18/german_pirate_party_uses_drone_to_crash_event_with_chancellor_angela_merkel.html.

Bureau of Justice Assistance. 2012. *Guide to Conducting Privacy Impact Assessments for State, Local and Tribal Justice Entities*. Washington, DC: Bureau of Justice Assistance. https://it.ojp.gov/documents/d/Guide%20to%20Conducting%20Privacy%20Impact%20Assessments_compliant.pdf.

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

Cape Breton Post. 2014. "Eye in the sky: Nova Scotia RCMP demonstrate new drone to be used by force." *Cape Breton Post*, July 23. http://www.capebretonpost.com/News/Local/2014-07-23/article-3809595/Eye-in-the-sky%3A-Nova-Scotia-RCMP-demonstrate-new-drone-to-be-used-by-force/1.

Clarridge, C. "Protesters steal the show at Seattle police gathering to explain intended use of drones." *The Seattle Times*, October 25. http://www.seattletimes.com/seattle-news/protesters-steal-the-show-at-seattle-police-gathering-to-explain-intended-use-of-drones/.

Cohen McCullough, D.R. (2014). "Unmanned aircraft systems (UAS) guidebook in development." *COPS Community Policing Dispatch* 7(8). http://cops.usdoj.gov/html/dispatch/08-2014/UAS_Guidebook_in_Development.asp.

Collinson, R.P.G. 2011. *Introduction to Avionics Systems*, 3rd ed. Dordrecht: Springer.

Coptaire. 2011. "Propellor Shroud Project." Message board post to DIYDrones.com. May 15, 2011. http://diydrones.com/profiles/blog/show?id=705844%3ABlogPost%3A400949&commentId=705844%3AComment%3A828253.

Crime Stoppers USA. 2015. "CSUSA profile." Accessed March 19, 2015. http://www.crimestoppersusa.com/profile.htm.

COPS Office (Office of Community Oriented Policing Services). 2012. *Community Policing Defined*. Last modified October 5, 2012. http://ric-zai-inc.com/ric.php?page=detail&id=COPS-P157.

DHS (Department of Homeland Security). 2015a. "DHS Financial Assistance." Last modified December 28, 2015. http://www.dhs. gov/dhs-financial-assistance.

———. 2015b. "Law Enforcement Resources." Last modified September 23, 2015. http://www.dhs.gov/law-enforcement-resources.

District DOT (Department of Transportation). 2005. District Of Columbia Amber Alert Plan. Washington, DC: District DOT. http://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/DC_amberalertplan.pdf.

Divis, D.A. 2013. "Homeland Security opens new round of small UAS evaluations" [online community post]. Last modified August 14, 2013. http://www.insidegnss.com/node/3666.

DJI. 2015. "Phantom aerial film multi rotor system with GoPro mount" [product page]. Accessed April 9, 2015. http://www.dji.com/product/phantom

DoD (U.S. Department of Defense). 2001. "Background Briefing on Unmanned Aerial Vehicles" [news briefing]. October 31. http://fas.org/irp/program/collect/uav_103101.html.

DoJ (U.S. Department of Justice). 2015. "Department of Justice establishes policy guidance on domestic use of unmanned aircraft systems" [press release]. Last modified May 22, 2015. http://www.justice.gov/opa/pr/department-justice-establishes-policy-guidance-domestic-use-unmanned-aircraft-systems.

Dow Chemical Co. v. U.S., 476 U.S. 227, 106 S. Ct. 1819, 90 L. Ed. 2d 226, 24 Env't. Rep. Cas. (BNA) 1385, 16 Envtl.L. Rep 20679 (1986).

Draganfly Innovation, Inc. 2015a. "Draganfly Training." Accessed April 16, 2015. https://www.draganfly.com/training/.

———. 2015b. "Handheld controller" [info sheet]. Accessed April 7, 2015. http://www.draganfly.com/uav-helicopter/ draganflyer-x6a/specifications/HHC_handheld_ controller_v6.pdf.

———. 2015c. "RCMP "F" Division Customer Spotlight." Accessed April 8, 2015. http://www.draganfly.com/our-customers/ customer_spotlight/RCMP_spotlight_v5.pdf.

———. 2015d. "Sony QX100 camera system with single axis stabilized camera mount" [product page]. Accessed April 7, 2015. http://www.draganfly.com/sku/DF-QX100I-1B. php5.

Envisage Technologies. 2014. "Drones may be the future of disaster relief." Last modified April 8, 2014. http://www.envisagenow.com/drones-may-be-the-future-of-disaster-relief/#sthash.jOtjUHir.dpbs.

Executive Office of the President. 2015. "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems." 80 FR 9355. https://www.federalregister.gov/articles/2015/02/20/2015-03727/promoting-economic-competitiveness-while-safeguarding-privacy-civil-rights-and-civil-liberties-in.

FAA (Federal Aviation Administration). 2013. *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap* (first edition). Washington, DC: FAA. https://nppa.org/sites/default/files/UAS_Roadmap_2013.pdf.

———. 2014a. "Certificates of waiver or authorization (COA)." Last modified November 14, 2014. https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/.

———. 2014b. *FAA Aerospace Forecasts FY 2014-2034*, Aviation Forecasts. Washington DC: FAA. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FAA_Aerospace_Forecasts_FY_2016-2036.pdf.

———. 2014c. "Operational Requirements For UAS." FAA Rule 8900.1, Vol. 16, Chapter 5, Section 3 16-5-3-7 E. June 23, 2014. Washington, DC: FAA. http://fsims.faa.gov/PICDetail.aspx?docId=8900.1,Vol.16,Ch5,Sec3.

———. 2014d. "Sporting event temporary flight restriction." FC NOTAM 4/3621, *Notices to Airmen* October 27, 2014. Washington, DC: FAA. http://tfr.faa.gov/save_pages/detail_4_3621.html.

———. 2015a. "DOT and FAA propose new rules for small unmanned aircraft systems [press release]." Last modified February 15, 2015. http://www.faa.gov/news/press_releases/news_story.cfm?newsId=18295.

———. 2015b. "Unmanned aircraft systems (UAS) frequently asked questions." Last modified December 18, 2015. https://www.faa.gov/uas/faq/#qn1.

———. 2015c. *Law Enforcement Guidance For Suspected Unauthorized UAS Operations*. Washington, DC: FAA. http://www.faa.gov/uas/regulations_policies/media/FAA_UAS-PO_LEA_Guidance.pdf.

———. 2015d. "Overview of Small UAS Notice of Proposed Rulemaking" [summary of major provisions of proposed part 107 in the FAA's small UAS NPRM]. Washington DC: FAA. http://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.

———. 2015e. "Petitioning for exemption under section 333." Last modified November 19, 2015. http://www.faa.gov/uas/legislative_programs/section_333/how_to_file_a_petition/.

———. 2015f. "Test Sites." Last modified August 4,2015. https://www.faa.gov/uas/legislative_programs/test_sites/.

———. 2015g. "Unmanned aircraft systems (UAS) regulations and policies." Last modified December 17, 2015. https://www.faa.gov/uas/regulations_policies/.

———. 2016. "*Authorizations granted via section 333 exemptions*." Last modified January 27, 2016. https://www.faa.gov/uas/legislative_programs/section_333/333_authorizations/.

Falcon Unmanned. 2015. "Falcon Unmanned pricing" [pricing page]. Accessed April 7, 2015. http://www.falconunmanned.com/falcon-prices/.

Farivar, C. 2015. "We know where you've been: Ars acquires 4.6M license plate scans from the cops." *Ars Technica*, March 24. http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/.

Florida v. Riley, 488 U.S. 455 (1989).

Fox Business. 2014. "Grand Forks County uses drones for 1st time at night when suspects flee after traffic stop." Last modified September 29, 2014. http://www.foxbusiness.com/markets/2014/09/29/grand-forks-county-uses-drones-for-1st-time-at-night-when-suspects-flee-after.html.

Gilligan, Margaret (Peggy). 2014. Testimony in *Hearing before the House Transportation and Infrastructure Committee, Subcomm. on Aviation, on U.S. Unmanned Aircraft Systems, Integration, Oversight, and Competitiveness*, 113th Cong. 84. https://fas.org/irp/congress/2014_hr/uas.pdf.

Goodman, M. 2013. "Criminals and terrorists can fly drones too." *Time*, January 13, 2013. http://ideas.time.com/2013/01/31/criminals-and-terrorists-can-fly-drones-too/.

Great Westchester Homeowners Assn' v. City of Los Angeles. 603 P.2d 1329 (Cal. 1979).

H.B. 255, 28th Legis. Assem. (Alaska 2014).

H.B. 296, 2015 Gen. Sess. (Utah 2015).

H.B. 912, 83rd Legis. Assem. Reg. Sess. (Tex. 2013).

H.B. 1009, 118th Gen. Assem. (Ind. 2014).

H.B. 1029, Legis. Assem. Reg. Sess. (La. 2014).

H.B. 1652, 9th Gen. Assem. (Ill. 2013).

H.B. 1952, 108th Gen. Assem. Reg. Sess. (Tenn. 2014).

H.B. 2012, 2013 Gen. Assem. (Va. 2013).

H.B. 2125, 2015 Gen. Assem. (Va. 2015).

H.B. 2710, 77th Legis. Assem. (Ore. 2013).

H.C.R. 217, 83rd. Legis. Assem. (Tex. 2013).

Herhold, S. 2014. "Big Brother, begone: The San Jose police should get rid of their drone." *San Jose Mercury News*, August 2. http://www.mercurynews.com/scott-herhold/ci_26264766/big-brother-begone-san-jose-police-should-get.

H.F. 2289. Gen. Assem. (Iowa 2014).

IACP (International Association of Chiefs of Police). 2012. *Recommended Guidelines For the Use of Unmanned Aircraft.* Arlington, Virginia: IACP.

———. 2014. *IACP Technology Framework*. Arlington, VA: IACP. http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.

Jansen, B. "New drone rules to include hobbyists." *USA Today*, October 19.

Joffe v. Google, 729 F.3d 1262 (9th Cir. 2013).

JustNet. 2016. "Technology Decision Tool." Accessed February 1, 2016. https://www.justnet.org/technology_decision_tool.html.

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

Kinnard, M. 2014. "Drone carrying contraband crashes at SC prison." *Tuscaloosa News*, July 30. http://www.tuscaloosanews.com/article/20140730/NEWS/140739983.

Koller, Annelie. 2014. "Terminator Was Not Open-source: How 3D printing and DIY drone community are changing perceptions." Blog post on DIYDrones.com. July 30, 2014. http://diydrones.com/profiles/blogs/terminator-was-not-open-source-how-3d-printing-and-diy-drone-1.

KPIX. 2015. "Calls for police drones renewed following shooting of SJPD officer." KPIX (SF Bay Area), March 26. http://sanfrancisco.cbslocal.com/2015/03/26/fatal-shooting-of-san-jose-police-officer-renews-conversation-on-drone-use/.

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

L.D. 25, 127th Legis. Assem. (Maine 2015).

Lerner, B. 2014. "UAVs and perimeter security in the private sector." Center for Security Policy. Last modified June 24, 2014. http://www.centerforsecuritypolicy.org/2014/06/24/uavs-and-perimeter-security-in-the-private-sector/.

Lopez, O. 2014. "DEA reveals cartels use drones to transport drugs from Mexico into US." *Latin Times*, July 10. http://www.latintimes.com/mexican-drug-war-news-dea-reveals-cartels-use-drones-transport-drugs-mexico-us-190217.

Lum, C., L. Merola, L., J. Willis, J., and B. Cave. 2010. *License Plate Recognition Technology (LPR): Impact Evaluation and Community Assessment*. Fairfax, VA: George Mason University, Center for Evidence Based Crime Policy. http://cebcp.org/wp-content/evidence-based-policing/LPR_FINAL.pdf.

McKenna, A.T. 2014a. *Overview of UAS/UAV-Related State Legislation*. Memorandum, July 31, 2014. Baltimore, MD: Silver McKenna.

———. 2014b. *Overview of UAS/UAV Technology and Regulation: Analysis of Police use of UAS/UAV systems Under U.S. Constitution and Case Law.* Memorandum, July 31, 2014. Baltimore, MD: Silver McKenna.

———. 2014c. *Police use of UAVs: Liability Analysis and Risk Management Considerations*. Memorandum, July 14, 2014. Baltimore, MD: Silver McKenna.

Measure, a 32 Advisors Company. 2015. American Farm Bureau Federation and Measure produce first ever report and calculator on value of drones in agriculture [press release]. Last modified July 21, 2015. http://measure32.com/measure-afbf-roicalculator-drones-precisionag/4.

Mesa County Sheriff's Office, Law Operations Division. 2015. "MSCO Unmanned Aircraft System Team Frequently Asked Questions." Accessed February 5, 2015. http://www.mesacounty.us/uav/.

Miller, Benjamin. 2013. Testimony in *The Future of Drones In America: Law Enforcement and Privacy Consideration: Hearing Before the Senate.Comm. on the Judiciary*, 113th Cong. 50. https://www.gpo.gov/fdsys/pkg/CHRG-113shrg81775/html/CHRG-113shrg81775.htm.

Monmouth University Poll. 2012. "U.S. supports some domestic drone use but public registers concern about own privacy." West Long Branch, NJ: Monmouth University. http://www.monmouth.edu/assets/0/32212254770/32212254991/32212254992/32212254994/32212254995/30064771087/42e90ec6a27c40968b911ec51eca6000.pdf.

NBC News. 2013. "Seattle cancels police drone program after outcry over privacy issues." Last modified February 8, 2013. http://usnews.nbcnews.com/_news/2013/02/08/16903237-seattle-cancels-police-drone-program-after-outcry-over-privacy-issues.

NCSL (National Conference of State Legislatures). 2015a. *2013 Unmanned Aircraft Systems (UAS) Legislation*. Last modified July 20, 2015. http://www.ncsl.org/research/transportation/2013-state-unmanned-aircraft-systems-uas-legislation.aspx.

———. 2015b. *2014 Unmanned Aircraft Systems (UAS) Legislation*. Last modified July 20, 2015. http://www.ncsl.org/research/transportation/2014-state-unmanned-aircraft-systems-uas-legislation.aspx.

————. 2016. *Current Unmanned Aircraft State Law Landscape*. Last modified August 16, 2016. http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx#1.

Nicks, D., and S. Grossman. 2014. "Space needle guests say drone crashed into window." *Time*, July 25. http://time.com/3033869/seattle-drone-space-needle/.

Norton, Congresswoman Eleanor Holmes (DC). 2015. "Norton says White House drone incident highlights need for further regulation" [press release]. Last modified January 26, 2015. http://norton.house.gov/media-center/press-releases/norton-says-white-house-drone-incident-highlights-need-for-further.

N.Y. v. Class, 475 U.S. 106 (1986).

OCHA (United Nations Office for the Coordination of Humanitarian Affairs). 2014. *Unmanned Aerial Vehicles in Humanitarian Response*. Occasional Policy Paper. OCHA Policy and Studies Series: June 2014. N.p: OCHA. https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf.

Ohio DOT (Department of Transportation). 2014. *Perimeter Security Operational Assessment for the Ohio Department of Rehabilitation and Corrections.* Columbus: State of Ohio DOT. http://www.dot.state.oh.us/Divisions/ContractAdmin/Contracts/PurchDocs/507-15.pdf.

PERF (Police Executive Research Forum). 2014. *Future Trends in Policing*. Washington, D.C.: Office of Community Oriented Policing Services.

Petroski, William. 2014. "Iowa Poll: 76% favor requiring warrants for drone surveillance." *Des Moines Register*, March 11. http://www.desmoinesregister.com/story/news/politics/2014/03/11/iowa-poll-76-favor-requiring-warrants-for-drone-surveillance/6311137/.

Pollack, J. 2014. "Cleveland, police host gun buyback event Saturday, offering to exchange gift cards and sports tickets." *NewsChannel 5* (Cleveland, Ohio), September 3. http://www.newsnet5.com/news/local-news/cleveland-metro/turn-handgun-into-police-saturday-and-get-gift-card-to-local-store.

President's Task Force on 21st Century Policing. 2015. *Final Report of the President's Task Force on 21st Century Policing*. Washington, DC: Office of Community Oriented Policing Services. http://www.cops.usdoj.gov/pdf/taskforce/TaskForce_FinalReport.pdf.

Rapp, Geoffrey. 2009. "Unmanned Aerial Exposure: Civil Liability Concerns Arising from Domestic Law Enforcement Employment of Unmanned Aerial Systems." *North Dakota Law Review* 85, 623-648. https://law.und.edu/_files/docs/ndlr/pdf/issues/85/3/85ndlr623.pdf.

RCAPA (Remote Control Aerial Platform Association). 2016. "RCAPA general guidelines." Accessed February 3, 2016. http://rcapa.net/guidelines/.

RCMP (Royal Canadian Mounted Police). 2013. "Single Vehicle Rollover – Saskatoon RCMP Search for Injured Driver with Unmanned Aerial Vehicle." Last modified May 9, 2013. http://www.rcmp-grc.gc.ca/sk/news-nouvelle/video-gallery/video-pages/search-rescue-eng.htm.

Repard, P. 2015. "Police chiefs group offers drone use policy." *The San Diego Union-Tribune*, May 20. http://www.utsandiego.com/news/2015/may/20/drones-unmanned-aircraft-iacp-law-enforcement/.

Reporters Committee for Freedom of the Press. 2015. "Access to police body camera videos: The wild west of open records requests." Last modified April 15, 2015. http://www.poynter.org/news/mediawire/335761/access-to-police-body-camera-videos-the-wild-west-of-open-records-requests/.

Rost, Robert. 2012. "Small Unmanned Aircraft System" [press release]. Grand Forks, ND: Grand Forks County Sheriff's Department. http://www.draganfly.com/pdf/Grand%20Forks%20County%20-%20Press%20Release.pdf.

RTI International. 2013. "New study shows public support use of unmanned aircraft systems." Last modified June 24, 2013. http://www.rti.org/newsroom/news.cfm?obj=62bdc848-5056-b100-0c6256d7f3203f25.

San Jose Police Department, Press Information Office. 2014. "San Jose police provide statement regarding purchase of unmanned aerial system (UAS)" [press release]. Last modified August 5, 2014. http://www.sjpd.org//inews/viewPressRelease.asp?ID=1874.

Santos, L.A. 2013. "In the Philippines, drones provide humanitarian relief." Last modified December 16, 2013. https://www.devex.com/news/in-the-philippines-drones-provide-humanitarian-relief-82512.

S.B. 92, 2013 Legis. Assem. (Fla. 2013).

S.B. 167, 2014 Gen. Sess. (Utah 2014).

S.B. 196, 63rd Legis. Assem. (Mont. 2013).

S.B. 196, 2013-2014 Legis. Assem. (Wis. 2014).

S.B. 796, 108th Gen. Assem. Reg. Sess. (Tenn. 2013).

S.B. 1134, 62nd Legis. Assem. (Idaho 2013).

S.B. 1301, 2015 Gen. Assem. (Va. 2015).

S.B. 1331, 2013 Gen. Assem. (Va. 2013).

S.B. 1587, 98th Gen. Assem. (Ill. 2013).

S.B. 1777, 108th Gen. Assem. Reg. Sess. (Tenn. 2014).

S.B. 2937, 98th Gen. Assem. (Ill. 2014).

Serna, J. 2014. "Anti-spying coalition launches campaign against LAPD drones." *Los Angeles Times*, August 21. http://www.latimes.com/local/lanow/la-me-ln-anti-drone-campaign-lapd-city-hall-20140821-story.html.

Sengupta, S. 2013. "Rise of drones in U.S. drives efforts to limit police use." *The New York Times*, February 15. http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?pagewanted=all&_r=1&.

Sherman, T. 2015. "How a free Army helicopter cost Newark police more than $2M." *NJ.com*, January 11. http://www.nj.com/news/index.ssf/2015/01/how_a_free_army_helicopter_cost_newark_police_more_than_2m.html.

Soaring Sky. 2015. "The advantages of using drone-powered land surveying equipment." Last modified November 3, 2015. https://soaringsky.net/2015/11/03/the-advantages-of-using-drone-powered-land-surveying-equipment/.

Stanley, J. and Crump, C. 2011. *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*. New York: American Civil Liberties Union. https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf.

Stone, J. 2014. "North Dakota police use drones to arrest fleeing drunk driving suspects." *International Business Times*, October 3, 2014. http://www.ibtimes.com/north-dakota-police-use-drone-arrest-fleeing-drunk-driving-suspects-video-1699066.

The Current Operations and Capital Improvements Appropriations Act of 2014, S.B. 744 section 7.16(e), 2013 Gen. Assem. (N.C. 2014).

United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987).

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

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

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

Unmanned Vehicle University. 2015. "UAV pilot certificate training." Accessed April 16, 2015. http://www.uxvuniversity.com/uav-pilot-training-certificate/.

Valenzuela, B. 2014. "Long Beach Police keeps helicopters flying as other departments ground theirs." *Press-Telegram Crime News*, January 1. http://www.presstelegram.com/general-news/20140101/long-beach-police-keeps-helicopters-flying-as-other-departments-ground-theirs.

Virginia Department of Criminal Justice Services. 2013. *Protocols for the Use of Unmanned Aircraft Systems (UAS) by Law-Enforcement Agencies*. House Document 12. Richmond: Commonwealth of Virginia.

Warwick, G. 2014. "FAA preparing phased integration of UAS over five years." *Aviation Week,* July 3. http://aviationweek.com/commercial-aviation/faa-preparing-phased-integration-uas-over-five-years.

Whitlock, C. 2014. "FAA will miss deadline to integrate drones in U.S. skies, report says." *The Washington Post*, June 30. http://www.washingtonpost.com/world/national-security/faa-will-miss deadline-to-integrate-drones-in-us-skies-report-says/2014/06/30/fd58e8e2-007f-11e4b8ff89afd3fad6bd_story.html.

WISTV. 2013. "City council unanimously approves drone aircraft." WISTV (Monroe, North Carolina), March 8. http://www.wistv.com/story/21538226/monroe-police-consider-purchase-of-unmanned-aircraft.

Wright, A. 2015. "Drones offer risks, underwriting challenges." *Risk & Insurance*, January 5. http://www.riskandinsurance.com/drones-offer-risks-underwriting-challenges/.

Yakabe, A. 2015. "UAS on Main Street: Policy and enforcement at the local level." *Homeland Security Affairs 11*(4), 1-27. https://www.hsaj.org/articles/4522.

About the Police Foundation

The Police Foundation is a national, nonpartisan, nonprofit organization dedicated to advancing innovation and science in policing. As the country's oldest police research organization, the Police Foundation has learned that police practices should be based on scientific evidence about what works best, the paradigm of evidence-based policing. Established in 1970, the foundation has conducted seminal research in police behavior, policy, and procedure, and works to transfer to local agencies the best new information about practices for dealing effectively with a range of important police operational and administrative concerns. Motivating all of the foundation's efforts is the goal of efficient, humane policing that operates within the framework of democratic principles and the highest ideals of the nation.

About the COPS Office

The Office of Community Oriented Policing Services (COPS Office) is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, territorial, and tribal law enforcement agencies through information and grant resources.

Community policing begins with a commitment to building trust and mutual respect between police and communities. It supports public safety by encouraging all stakeholders to work together to address our nation's crime challenges. When police and communities collaborate, they more effectively address underlying issues, change negative behavioral patterns, and allocate resources.

Rather than simply responding to crime, community policing focuses on preventing it through strategic problem solving approaches based on collaboration. The COPS Office awards grants to hire community police and support the development and testing of innovative policing strategies.

COPS Office funding also provides training and technical assistance to community members and local government leaders, as well as all levels of law enforcement. The Collaborative Reform Initiative for Technical Assistance (CRI-TA), a program that promotes organizational transformation through analysis of policies, practices, and training related to issues of concern, is also available to law enforcement agencies

Since 1994, the COPS Office has invested more than $14 billion to provide training and technical assistance, enhance crime fighting technology, and add more than 125,000 officers to our nation's streets. We also offer a wide variety of information resources to help law enforcement and community leaders address specific crime issues at www.cops.usdoj.gov.

Technology has provided numerous benefits to law enforcement, increasing operational efficiency as well as officer and public safety. And with the growing use of unmanned aircraft systems (UAS) by law enforcement, these advantages have increased exponentially.

But operating a UAS safely, without violating privacy and other civil rights, presents great challenges too. And the public is wary. Many people worry about "spying," unwanted surveillance, and data collection.

In response, the Police Foundation has developed this one-of-a-kind guidebook to help agencies decide whether to acquire a UAS, and if they do, how to develop policies and procedures which will ensure public support, avoid potential pitfalls, and build community trust. A comprehensive guide to all aspects of this technology, Community Policing and Unmanned Aircraft Systems: Guidelines to Enhance Community Trust provides information on UAS training, staffing, policy development, funding, regulations and more–all with a focus on community collaboration and buy-in.

COPS
Community Oriented Policing Services
U.S. Department of Justice

U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street NE
Washington, DC 20530

To obtain details about COPS Office programs, call the COPS Office Response Center at 800-421-6770.

Visit the COPS Office online at **www.cops.usdoj.gov**.

POLICE FOUNDATION

Police Foundation
1201 Connecticut Ave NW, Suite 200
Washington, DC 20036-2636

www.policefoundation.org

e011607738
Published 2016