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.

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.

- 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;

- 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.