DHS Privacy Suggestions on Agency Drone Programs

As technology continues to blur the lines between privacy and security, the Homeland Security Department has several suggestions to help agencies consider civil rights and liberties issues when setting up their respective unmanned aircraft system programs.

The DHS Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group, which department leaders formed about three years ago, released 15 best practices for agencies as they establish their own unmanned aircraft systems (UAS) or drones.

Co-chairs of the working group acknowledged that all suggestions might not apply to every agency. But DHS — specifically CBP — can draw on 10 years of experience from using unmanned aircraft to protect U.S. borders, they wrote.

"The DHS Working Group neither proposes nor intends that this document regulate any other government entity," the co-chairs wrote in a joint statement. "Our goal, rather, is simply to share the best practices we have identified as helping to sustain privacy, civil rights and civil liberties throughout the lifecycle of an unmanned aircraft systems program."

The group includes DHS Officer for Civil Rights and Civil Liberties Megan Mack, DHS Chief Privacy Officer Karen Neuman and Customs and Border Protection Deputy Assistant Commissioner Edward Young.

Many of the group's recommendations serve as reminders to agencies that as they begin to establish UAS programs, they keep privacy, civil liberties and rights experts involved throughout the entire implementation process — from the procurement to audit and oversight stages.

Agencies should, for example, regularly keep track and submit reports to their legal, privacy, civil rights and civil liberties experts on all of their UAS activities and the complaints they receive.

Other suggestions center around the issue of information sharing and security.

Before setting up a UAS program, the group suggests some agencies conduct a Privacy Threshold Analysis to determine whether their programs will conduct personally identifiable information (PII).

Agencies should also set up security safeguards to prevent data loss or unauthorized access to PII.

"Security measures should be layered to avoid reliance on any single security measure," the working group said. "Employ several measures that functionally overlap to create redundancy in the security of data and the overall program."

But the guidelines lack specifics on how long agencies can store information about individuals, which Neema Singh Guliani, legislative counsel at the American Civil Liberties Union, said is a problem.

The working group, for example, suggests agencies establish an approved records retention schedule that would systematically get rid of the information that is no longer useful or legal to keep.

"Ensure retention periods are compatible with the type of data retained and needs of the unmanned aircraft program," the group suggested. "Data collected that does not pertain to an authorized purpose should not be retained beyond 180 days."

But Singh Guliani said agencies could do a lot with that information in 180 days. If one agency uses a drone to collect information for a specific, authorized purpose and holds that data for 90 days, it could give another organization that same information, she said.

U2

"Right now, if you have information for an authorized purpose — whatever that means — and throughout the course of that you want to use if for another purpose, there's nothing that says you can't do that," Singh Guliani said.

The 15 best practices are:

1. Consult legal counsel, privacy and civil rights and liberties experts at each step in the formation process.
2. Publicly state the purpose for setting up an unmanned aircraft system program.
3. Publicly document any changes to the program's purpose.
4. Put a senior official, preferably one in an agency's privacy and civil liberties office, in charge of overseeing the program.
5. Consult privacy and civil liberties experts throughout the implementation process.
6. Conduct an analysis of possible privacy and civil liberties concerns before establishing a program.
7. Limit the data and information that unmanned aircraft systems collect and keep, and comply with records retention policies.
8. Respect constitutional activities.
9. Set up a redress program that can receive, investigate and address privacy, civil liberties and rights complaints.
10. Establish audits and other accountability procedures.
11. Design the UAS with the proper security controls to ensure that the right data stays in the proper place.
12. Include legal, privacy and civil rights considerations in the procurement process.
13. Maintain a transparent and open relationship with the public about the UAS and its implementation.
14. Train personnel on privacy and civil liberties issues that may come up when operating an unmanned aircraft system.
15. Develop a system for handling UAS service requests.

Though the recommendations are intended for federal, state and local agencies, as well as government partners and grantees, the private sector might also find them useful, the co-chairs wrote.

Source: Federal News Radio

U.S. Department of Homeland Security

Best Practices for

Protecting Privacy, Civil Rights & Civil Liberties

In

Unmanned Aircraft Systems Programs

U.S. Department of Homeland Security
Privacy, Civil Rights & Civil Liberties
Unmanned Aircraft Systems Working Group

December 18, 2015

04

Joint Statement

Co-Chairs

Department of Homeland Security
Privacy, Civil Rights & Civil Liberties
Unmanned Aircraft Systems Working Group

As co-chairs of the Department of Homeland Security's (DHS) Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group (DHS Working Group), we are pleased to present these best practices, which reflect DHS' experiences in building unmanned aircraft system programs founded on strong privacy, civil rights, and civil liberties protections. Unmanned aircraft systems are an essential tool in DHS's border security mission and present a great deal of promise for assisting first responders and improving situational awareness.

These best practices represent an optimal approach to protecting individual rights that is influenced by U.S. Customs and Border Protection's (CBP) ten years of experience using unmanned aircraft systems as a tool in protecting and securing the Nation's borders. We are sharing these reflections broadly, recognizing that government entities (including CBP) have various limitations based upon their respective missions, operating characteristics, and legal authorities, and that many of the considerations that apply to our agency may not be applicable or appropriate for other entities. The DHS Working Group neither proposes nor intends that this document regulate any other government entity. Our goal, rather, is simply to share the best practices we have identified as helping to sustain privacy, civil rights, and civil liberties throughout the lifecycle of an unmanned aircraft systems program.[1]

We provide these best practices to share DHS's view of how to protect individual rights in this evolving technology-driven field. The rapid changes in technology compel legal, privacy, and civil rights and civil liberties experts to continually review and update implementing documents (e.g., best practices, standard operating procedures, and policies) to properly reflect changes in the law, as well as advances in the technology and new applications of the technology. It is important for government entities to ensure that technology is not used in a manner that erodes or violates an individual's statutory or constitutional rights.

[1] This guidance is intended for first responders (*e.g.*, emergency management, emergency medical service, fire departments, and security professionals responding to disasters and other emergencies), and does not seek to provide guidance in regard to investigative use of unmanned aircraft systems. DHS's primary experience with UAS operations, which serves as the basis for these best practices, has come in the context of general border surveillance operations.

Finally, even though these best practices are intended for DHS and our local, state, and federal government partners and grantees, the private sector may also find these recommendations valuable and instructive in creating their unmanned aircraft system programs.

Sincerely,

Megan H. Mack
Officer for Civil Rights
and Civil Liberties

Karen Neuman
Chief Privacy Officer

Edward B. Young
Deputy Assistant Commissioner
U.S. Customs and Border Protection

U.S. Department of Homeland Security

Best Practices for

Protecting Privacy, Civil Rights & Civil Liberties
In
Unmanned Aircraft Systems Programs

Overview

The term "unmanned aircraft systems" is used to define an unmanned aircraft and associated elements (including communication links and the 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.[1] In the past, unmanned aircraft were referred to as "unmanned aerial vehicles," but today they are simply referred to as unmanned aircraft.

Unmanned aircraft systems offer a variety of benefits for protecting our borders; supporting law enforcement; assisting in search and rescue operations; locating forest fire hot spots; evaluating dangerous environments (e.g., post-chemical spill and radiological exposure); conducting forensic imagery; inspecting pipeline and utilities; monitoring evacuation routes; and relaying telecommunication signals.[2]

The development of a new technology, significant improvement of a current technology, or the new application of an existing technology often results in concerns about the impact on individual privacy, civil rights, and civil liberties. For instance, the integration of government and commercial unmanned aircraft systems into the National Airspace System by 2015, as required by the *Federal Aviation Administration Modernization and Reform Act of 2012,* has prompted questions about how this might impact individual rights.[3]

In this regard, the Acting Officer for Civil Rights and Civil Liberties, the Acting Chief Privacy Officer, and the Assistant Commissioner for U.S. Customs and Border Protection, Office of Air and Marine jointly established the DHS *Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group* (DHS Working Group) in September 2012 to "provide leadership to the homeland security enterprise by clarifying the privacy, civil rights, and civil liberties legal and policy issues surrounding government use of [Unmanned Aircraft Systems]."[4]

---

[1] *FAA Modernization and Reform Act of 2012*, Pub. L. No.112-95.

[2] Government Accountability Office, *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, p. 10, GAO-12-981 (September 2012).

[3] *Id.* at 2-3, 32-36.

[4] *Memorandum for the Secretary, Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (UAS),* from Tamara J. Kessler, Acting Officer, Office for Civil Rights and Civil Liberties; and Jonathan R. Cantor, Acting Chief Privacy Officer *(September 12, 2012).* The DHS *Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group,* co-chaired by the DHS Office for Civil Rights & Civil Liberties, DHS Privacy Office and U.S. Customs and Border Protection, is comprised of policy and operational subject matter experts from across DHS including the U.S. Coast Guard, Office of Intelligence and Analysis, Office of the General Counsel, Office of Policy, National Protection and Programs

67

The DHS Working Group publishes these best practices to inform DHS and our local, state, and federal government partners and grantees that want to establish unmanned aircraft programs based on policies and procedures that are respectful of privacy, civil rights, and civil liberties. These best practices are also consistent with the February 15, 2015 Presidential Memorandum: *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*.[5]

Unmanned aircraft systems programs are encouraged to incorporate principles of transparency and accountability, while not revealing information that could reasonably be expected to compromise law enforcement or national security, and consider the issues that DHS has encountered in the context of developing its own policies and programs.

These best practices are not prescriptive, but rather are provided to share the Department's considerable experience operating unmanned aircraft systems in securing the Nation's borders and supporting communities during natural disasters and emergencies, and to provide unmanned aircraft system operators with privacy, civil rights, and civil liberties practices to consider before initiating an unmanned aircraft program. The applicability or advisability of implementing each recommended practice to a particular unmanned aircraft program will vary based upon each individual agency's legal authorities, purpose of the mission, mission of the agency, type of unmanned aircraft system, type of payload onboard, operating characteristics, and flight profiles. Therefore, each agency is encouraged to consult with its legal counsel to ensure compliance with its agency's own particular legal requirements

Although the intended audience is DHS and other government agencies, the private sector may also find these practices instructive in creating or operating unmanned aircraft programs.

It is important that agencies work closely with legal, privacy, civil rights, and civil liberties experts to ensure compliance with applicable local, state, and federal laws and regulations when developing an unmanned aircraft program.

Directorate, Science &Technology Directorate, Federal Emergency Management Agency and the Office of Operations Coordination and Planning.

[5] Presidential Memorandum, *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (2015). http://wh.gov/ibmmJ.

Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs

1. **Consult Your Legal Counsel, Privacy, Civil Rights, and Civil Liberties Experts to Ensure Legal Authority and Compliance**

   Prior to establishing an unmanned aircraft program, work closely with your legal counsel to confirm there is legal authority to operate unmanned aircraft systems for the intended purpose and whether it is permissible to fly unmanned aircraft in the desired area. Involve legal, privacy, civil rights, and civil liberties experts at every stage of formulation, operation, and review of an unmanned aircraft program to ensure compliance with applicable laws and policies.

2. **Clearly State the Purpose of the Unmanned Aircraft Program**

   Clearly articulate the primary purpose for establishing the unmanned aircraft systems program.

   Considerations:

   - The public may better understand and appreciate an agency's reasons for establishing an unmanned aircraft program with a clearly stated and plainly worded purpose.
   - Identify the challenge that prompted your agency to create an unmanned aircraft program and how unmanned aircraft systems will assist in addressing that challenge.
   - Determine the appropriate payload(s) (e.g., infrared camera, video, radar) for each stated purpose.
   - Describe the primary purpose(s) of your unmanned aircraft program online and/or make this information publicly accessible, while not revealing information that could reasonably be expected to compromise law enforcement or national security.

3. **Stay Focused on the Purpose of the Unmanned Aircraft Program**

   Recognizing that the purpose and utility of a UAS program may evolve over time, certain changes to the unmanned aircraft program's stated purpose that may impact individual rights should be reviewed by an agency's legal, privacy, civil rights and civil liberties experts.

   Consideration:

   - Changes to the unmanned aircraft program's primary purposes should be reflected in documents readily available to the public prior to implementing those changes (if feasible).

4. **Designate an Individual Responsible for Privacy, Civil Rights, and Civil Liberties Compliance**

   This should be a senior level individual within the organization, preferably in the office(s) responsible for privacy, civil rights and civil liberties (if one exists), with working knowledge of the relevant privacy, civil rights, and civil liberties laws and regulations. The senior level individual should have a "direct line" to the person who has overall responsibility for the unmanned aircraft program.

5. **Stay Involved from Conception Throughout Deployment and Thereafter**

Program managers, technical staff, and operations staff should consult with legal, privacy, civil rights, and civil liberties experts throughout the lifecycle of the unmanned aircraft program.

Considerations:

- Establish and make publicly available clear policies and procedures to ensure respect for privacy, civil rights, and civil liberties while also making it clear that some information may not be able to be made publicly available based upon other legal, investigative or operational security reasons.
- Unmanned aircraft program managers should consult with legal, privacy, civil rights, and civil liberties experts when formulating concepts of operations, standard operating procedures, agreements, procurement contracts, and other underlying unmanned aircraft system documents.
- Establish a routine program review process to assess whether the program's purpose is being met and whether modifications are required. For example, the Presidential Memorandum: *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* requires federal agencies to perform such an assessment at least every three years and before new UAS programs are developed.

6. Conduct a Privacy Impact Assessment and Document Privacy Compliance

Agencies should conduct an analysis of potential privacy, civil rights, and civil liberties concerns before using unmanned aircraft systems. The Presidential Memorandum (referenced above) requires that Federal agencies examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS at least every three years, to ensure that privacy, civil rights, and civil liberties are protected. Although not required for all agencies, DHS found it useful to use a Privacy Impact Assessment (PIA) format for its examination—similar to that required for federal government information technologies under the *E-Government Act of 2002*. Privacy assessments are beneficial in evaluating an agency's compliance with applicable legal, regulatory, and policy requirements. The decision as to when such an assessment is appropriate will be a contextual decision for agencies to make based on their expertise, and the facts and circumstances involved. Any privacy assessment should identify potential risks to privacy, as well as steps an agency will take to mitigate any potential privacy risks. DHS has also found the PIA format useful for public notification of its UAS activities. For more information on the PIA format used by DHS (and to consult DHS PIAs that cover both unmanned aircraft systems and the use of sensors by aircraft) please visit the DHS Privacy Office webpage, available at http://www.dhs.gov/privacy-compliance.

Considerations:

- Some agencies conduct a brief Privacy Threshold Analysis to determine whether any Personally Identifiable Information[2] is to be collected or whether an unmanned

[2] DHS defines "Personally Identifiable Information" as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

TD

aircraft program raises privacy sensitivities before initiating a Privacy Impact Assessment.

- Consult state, local, and tribal or territorial laws to decide if any public notice is required regarding the system used to store, use, or share information acquired through unmanned aircraft systems. Federal agencies should consult the Privacy Act of 1974, as it may be applicable.

7. **Limit Collection, Use, Dissemination, and Retention of Unmanned Aircraft System-Recorded Data**

Collection, use, dissemination, and retention of unmanned aircraft system-recorded data should be limited to data legally acquired and relevant to the entity's operations. *See Best Practice #3.*

Considerations:

- Recorded images of individuals should not be retained beyond a reasonable period as defined by existing agency/departmental policy unless there is authorization based on a legal, policy or operational purpose.
- Collection, use, dissemination, or retention of unmanned aircraft system-recorded data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.
- The users of unmanned aircraft system-recorded data are responsible for ensuring dissemination of data is authorized and consistent with the recipients' legitimate need to know and authority to receive such data; any further dissemination by a data recipient should require the data owner's prior consent, which should only be provided upon the advice of the entity's legal counsel.
- Federal agencies need to establish whether their systems collect and store PII, and if so, whether there is an applicable System of Records Notice. Additionally, if their system does collect and store PII, agencies should consider whether they should limit the collection of personally identifiable information in accordance with OMB M 7-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.[3]
- Requests for unmanned aircraft system data by commercial entities, civil litigants, or Freedom of Information Act requesters should be reviewed by legal counsel to determine if such sharing is appropriate and permissible under applicable laws or regulations.
- Unmanned aircraft program managers should employ reasonable technological or administrative safeguards to ensure that images of people incidentally recorded who are not relevant to an operation are not disseminated or viewed unnecessarily to protect individual rights. This is especially important for recordingsthat include images of minors not relevant to an operation.
- Follow and clarify (if necessary) existing procedures for identifying, disseminating, retaining, indexing, and storing relevant and necessary unmanned aircraft system-recorded data in a retrievable manner.

[3] OMB M 7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (2007)*. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

- Establish or comply with an approved records retention schedule that systematically eliminates stored data after they are no longer legally required or operationally useful if not already present, this schedule should be periodically reviewed and updated. Ensure retention periods are compatible with the type of data retained and needs of the unmanned aircraft program. Data collected that does not pertain to an authorized purpose should not be retained beyond 180 days.

8. Respect Constitutionally Protected Activities

At times, government agencies may find it necessary to deploy unmanned aircraft systems to protect the public safety or respond to emergencies while other constitutionally protected activities may be taking place at the same location.

Considerations:

- Incidental images of identifiable individuals that are recorded, but not needed for legal compliance or law enforcement purposes, should be deleted according to established procedures and within 180 days.
- Be attuned to the potential privacy risks or legal ramifications arising from inadvertently capturing images of individuals engaging in constitutionally protected activities, and establish appropriate guidelines and administrative controls to anonymize, destroy, safeguard or prevent the misuse of such data, consistent with applicable law.
- Unmanned aircraft system-recorded data should not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations).

9. Have a Redress Program for Individuals that Covers Unmanned Aircraft System Activities

A robust and streamlined redress program is essential for permitting challenges to alleged inappropriate capture of personally identifiable information. Ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

Considerations:

- Where an administrative process is used, the process for resolving complaints should promote resolution within a reasonable amount of time.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security, individuals should be provided information regarding the factual basis for redress determinations.
- Information on how an individual requests redress should be succinct, straightforward, and readily available to the public.

10. Ensure Accountability in Management of Unmanned Aircraft Program

Accountability is a key element to a successful unmanned aircraft program. A program that properly records access and use of unmanned aircraft system-recorded data is better prepared to identify and resolve problems, and is more responsive to the public and regulatory bodies.

Considerations:

- Establish or confirm that existing oversight procedures (including audits or assessments) ensure compliance with policies and regulations; this may also serve as another layer of security and improve the overall integrity of the program.
- Provide adequate supervision of personnel and a process for personnel to report suspected cases of misuse or abuse.
- Impose penalties for misuse and non-compliance with policies and procedures.
- Establish policies and procedures for documenting individuals accessing or requesting access to unmanned aircraft system-recorded data.
- Institute a schedule of regularly submitted reports to agency legal, privacy, civil rights, and civil liberties experts documenting all unmanned aircraft system activities and complaints received during the prior reporting period. Reports should be submitted at least annually.
- Determine whether there is a need for new data sharing agreements, and establish appropriate record management policies before sharing data with other agencies.

11. Properly Secure and Store Unmanned Aircraft System-Recorded Data

An unmanned aircraft program should be designed with appropriate security safeguards to prevent or mitigate data loss, unauthorized access, use and disclosure of data.

Considerations:

- Ensure access to unmanned aircraft system-recorded data is controlled by using appropriate physical, personnel or technical security measures as appropriate (e.g., digital watermarks, encryption, or other security and authentication techniques) to protect the data.
- Apply appropriate handling and safeguarding procedures to unmanned aircraft system-recorded data that may be linked to individuals, or to sensitive information that is not otherwise personally identifiable (e.g., sensitive government or business proprietary information).
- Ensure the unmanned aircraft program authenticates and establishes a chain-of-custody that preserves the integrity of all data stored in the event that the data are produced in litigation.
- Develop procedures to ensure the system and its stored data are used only as authorized.
- Security measures should be layered to avoid reliance on any single security measure; employ several measures that functionally overlap to create redundancy in the security of data and the overall program.
- Protect the physical security of the communication links, and operational and data storage centers.
- Individuals with access to unmanned aircraft systems should receive background checks in accordance with an agency's regulations.

12. Review Agency Procurement Solicitations

Agencies should consult their legal, privacy, civil rights, and civil liberties experts when reviewing unmanned aircraft system sensor technology procurement solicitations to determine if the technology impacts individual rights (e.g., capable of observing non-public activities).

Considerations:

- Work with unmanned aircraft system vendors, payload vendors, and field operators to ensure that only equipment capabilities needed to support a specified purpose are used.
- Prior to any acquisition, ensure that the prospective sensor aligns with and furthers the purpose of the unmanned aircraft program, while minimizing the potential risk upon use to privacy, civil rights, or civil liberties.

13. Transparency and Outreach

Public support is essential for an unmanned aircraft program's success. A program that is not transparent according to applicable laws, agency policies, and best practices may quickly lose support and create misperceptions about the program's intended mission(s).

Considerations:

- When organizing initial outreach efforts, consider using the best practices listed in this guide that are operationally and legally feasible for your agency as a starting point, and periodically engage the public to keep them informed about the program and proposed significant changes.
- Outreach efforts should consider how to include persons with limited English proficiency and persons with disabilities.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security,, provide notice to the public as to where unmanned aircraft routinely operate (e.g., a description of the general operating area on websites, public documents, or through use of public signs).

14. Train Personnel

Require that personnel receive training regarding privacy and civil liberties policies that may apply to unamanned aircraft system operations. The agency's office(s) generally responsible for privacy, civil rights, and civil liberties should participate in developing and conducting the annual training.

Considerations:

- Individuals with access to stored data should receive training designed for the specific software and hardware employed by the agency's unmanned aircraft program.
- Those personnel responsible for handling unmanned aircraft systems support requests from other agencies should receive additional training on the agency's standard operating procedures for handling such requests.
- Staff should be instructed not to use any unmanned aircraft systems-acquired data for personal use.

15. Develop Procedures to Handle Unmanned Aircraft Systems Support Requests

The desirability and versatility of unmanned aircraft may prompt requests by outside organizations seeking unmanned aircraft systems support from an agency.

Considerations:

- Unmanned aircraft system assets used within the National Airspace System in support of an outside agency's request should only be operated by the agency authorized to operate unmanned aircraft by the Federal Aviation Administration.
- Establish and publish guidelines for agencies making unmanned aircraft systems support requests so that each requesting agency is aware of existing support limitations, and exactly what information they must provide to the unmanned aircraft systems operator.
- Ask sufficient questions of the requesting agency to ensure the scope and breadth of the request is understood so an appropriate payload and asset, which may be other than an unmanned aircraft (e.g., manned rotary- or fixed-wing aircraft), is provided to support the requesting agency.
- Agencies should create standard operating procedures for handling requests during both exigent and non-exigent circumstances.
- Standard operating procedures should (at a minimum) be reviewed by agency legal, privacy, civil rights, and civil liberties experts on an annual basis.
- It may be beneficial to have a memorandum of understanding or a similar written agreement that identifies each agency's roles and responsibilities in fulfilling a request. This agreement may include identifying which agency will exercise ownership, retention, and dissemination rights over any recorded data. It is best to create a template for support agreements that is then tailored to reflect each new request.
- If a request is received from other government agencies, there should be an understanding and respect for each agency's authorities and jurisdiction in fulfilling the request. If feasible, include an accounting of support requests received by, and responses from, the unmanned aircraft program (e.g., granted, denied, or asset other than an unmanned aircraft provided) when meeting periodic reporting requirements. *See Best Practice #10.*

Politics

Judge dismisses charges against man who shot down a drone for snooping on his daughter

By Aaron Sankin

Oct 30, 2015, 12:07pm CT | Last updated Oct 30, 2015, 12:28pm CT

http://bit.ly/1MxMnmS

Daily Dot Politics

Follow

A Kentucky judge ruled earlier this week that a man who shot down a drone flying over his property was acting within his rights.

William Meredith of Hillview, Kentucky, had insisted that the drone was spying on his 16-year old daughter, who was sunbathing in the backyard. Judge Rebecca Ward of the Bullitt District Court evidently agreed that Meredith had cause to fire at the UAV, because she dismissed charges of wanton endangerment and criminal mischief filed by the drone's owner David Boggs.

Boggs claimed that he was using the done to take pictures of another house close Meredith's. His $1,800 drone crashed into a nearby field after Meredith's shots hit it.

"Well, I came out and it was down by the neighbor's house, about 10 feet off the ground, looking under their canopy that they've got in their backyard...I went and got my shotgun and I said, 'I'm not going to do anything unless it's directly over my property,'" Meredith told local news station WDRB. "Within a minute or so, here it came. It was hovering over top of my property, and I shot it out of the sky."

A central question in the case was the height at which Boggs's drone was hovering above Meredith's residence. Boggs offered flight data from the drone showing that it had flown nearly 200 feet above Meredith's property.

"You will see now that we did not go below this altitude—we even went higher—nor did we hover over their house to look in," Boggs told WDRB. "And for sure didn't descend down to no 10 feet, or look under someone's canopy, or at somebody's daughter."

In her decision, Judge Ward noted that multiple witnesses claimed to have seen the drone flying below the tree line. That, she said, indicated that Boggs's drone use had been an invasion of Meredith's privacy.

While there is no law against shooting drones out of the sky, the Federal Aviation Administration would prefer if people didn't do so. "Shooting at aircraft poses a significant safety hazard," an agency official told CNET. "An unmanned aircraft hit by gunfire could crash, causing damage to persons or property on the ground, or it could collide with other objects in the air."

The Kentucky incident isn't the first high-profile drone-shootdown case. A New Jersey man was arrested last year for riddling his neighbor's drone with holes.

Drone laws vary considerably from state to state. A few days before the ruling in the Kentucky case, state Rep. Diane St. Onge introduced a bill to make "drone harassment" a misdemeanor in the state.

Sen. Rand Paul (R-Ky.), a 2016 presidential candidate, has also joined the fray, telling CNN that anyone who flies a drone over his home "better beware, because I've got a shotgun."

Federal law is unclear on the rights of property owners versus drone operators, because there is no set altitude at which personal property gives way to the commons of the air.

77

The last time the U.S. Supreme Court directly addressed the question was in the 1948 case *United States v. Causby*, in which the court found that a North Carolina farmer had no legal right to stop the airplanes from a nearby airport from flying over his house and scaring his chickens. The planes, the Court ruled, were flying high enough over his property that he couldn't claim dominion over activity in that airspace.

Drones fly far lower than 1940s aircraft, so the question of when they intrude on personal property is still open.

If you'd rather avoid pulling out your Beretta when you hear a buzzing overhead, you could sign up for No Fly Zone, a free service that works with drone manufacturers to register airspace where their drones cannot fly.

Photo via Don McCullough/flickr (CC BY 2.0) | Remix by Max Fleishman

http://bit.ly/1MxMnmS

Daily Dot Politics

Follow

From the Web

78

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF KENTUCKY
LOUISVILLE DIVISION
Electronically filed

JOHN DAVID BOGGS,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No.** 3:16-cv-6-DJH
	)	
WILLIAM H. MERIDETH,	)	
	)	
Defendant.	)	

COMPLAINT FOR DECLARATORY JUDGMENT AND DAMAGES

For his Complaint for Declaratory Judgment and Damages against Defendant, Plaintiff, John David Boggs, alleges the following:

INTRODUCTION

This case involves the intentional downing of Plaintiff's unmanned aircraft by Defendant. Plaintiff was flying his aircraft within Class G airspace and was neither trespassing nor invading anyone's privacy. Defendant has argued to the media and the courts that he was justified in using physical force to prevent what he perceived as an invasion of privacy and trespass upon his property. A state district court judge, dismissing criminal charges against Defendant, ruled that Defendant acted "within his rights." This turn of events has set the stage for a conflict between state-based claims of trespass to property, invasion of privacy, and trespass to chattles and long standing exclusive federal jurisdiction over the national airspace and the protection of air safety. The tension between private property rights and right to traverse safely the national airspace was resolved during the formative days of manned aviation. The issue is now arising in the context of unmanned aircraft, also known as "drones." Plaintiff seeks a declaratory judgment from this

79

Court to resolve that tension and define clearly the rights of aircraft operators and property owners.

PARTIES

1. Plaintiff, John David Boggs, is a resident of Bullitt County Kentucky.

2. Defendant, William H. Merideth, is a resident of Bullitt County Kentucky.

JURISDICTION AND VENUE

3. This is an action for a declaratory judgment, pursuant to 28 U.S.C. § 2201, for the purpose of determining a question of actual controversy between the parties as more fully appears below. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action involves issues arising from the laws of the United States. The supplementary state law claims underlying this case implicate significant federal issues. More specifically, plaintiff's right to relief as well as the defendant's defenses, will necessarily require resolution of a substantial question of federal law, to wit, the boundaries of the airspace surrounding real property, the reasonable expectation of privacy as viewed from the air, and the right to damage or destroy an aircraft in-flight, in relation to the exclusive federal regulation and protection of air safety, air navigation, and control over the national airspace.

The Court has supplementary jurisdiction over Plaintiff's claim arising under state law, pursuant to 28 U.S.C. § 1367, because that claim is part of the same case or controversy.

4. Venue is proper in this Court, pursuant to 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to the claim occurred in this District.

FACTUAL ALLEGATIONS

5. The Federal Aviation Administration ("FAA") has the exclusive authority to govern airspace within the United States and the operation of aircraft. The federal government's

80

interest in regulating aviation is paramount. Federal statutes and regulations, including the Transportation Laws of the United States, 49 U.S.C.A. § 40101 *et seq.*, and the Airline Deregulation Act, 49 U.S.C.A. § 41713, and the regulations promulgated by the Federal Aviation Administration pursuant to those laws, preempt state law in that area.

6. The FAA's airspace designations state that Class G airspace includes uncontrolled airspace that does not fall within any other classification between the surface and any overlying Class E airspace. Class G airspace is part of the navigable airspace the regulation of which substantially affects interstate commerce.

7. The FAA defines an "aircraft" as "a device that is used or intended to be used for flight in the air." 14 C.F.R. § 1.1.

8. On July 26, 2015, Plaintiff was operating by wireless controller an unmanned aircraft (also referred to as a "drone") at an altitude of approximately 200 feet above ground level in Class G airspace over Bullitt County, Kentucky.

10. Plaintiff's aircraft contained an onboard camera capable of recording video and still photographs. Plaintiff's aircraft recorded video of the horizon, woods and the rooftops of various houses. At no time was Plaintiff capturing video or still images of Defendant or anyone on his property. Below is the last image recorded by the aircraft prior to being shot by Defendant:

81

11. After approximately two minutes of flight, Defendant shot Plaintiff's unmanned aircraft down with a shotgun, resulting in damage to Plaintiff's property. Defendant later alleged that Plaintiff's unmanned aircraft may have been taking video or still images of Defendant's daughter while hovering over Plaintiff's property, thus Defendant asserts he was protecting his family's privacy rights and preventing further trespass.

12. Defendant was charged by Kentucky authorities with felony wanton endangerment and criminal mischief. On October 26, 2015, Kentucky District Court Judge Rebecca Ward dismissed the criminal charges against Defendant saying that Defendant "had a right to shoot" at the aircraft.

13. Defendant, using the nickname "The Drone Slayer," continues to assert that he was justified in shooting Plaintiff's aircraft and vows to do it again, as evidenced by his Facebook page:

https://www.facebook.com/william.merideth.7

14. Indeed, Defendant has implicitly encouraged others to engage in the same conduct by selling shirts depicted below:

82

15. Given the foregoing, Plaintiff requests a declaratory judgment, as set forth in more detail below.

FIRST CLAIM FOR RELIEF
(Declaratory Judgment)

16. Plaintiff incorporates by reference the allegations in the foregoing paragraphs as though fully set forth.

17. An actual controversy has arisen and now exists between Plaintiff and Defendant concerning their respective rights and obligations with respect to the damage caused to Plaintiff's aircraft by Defendant.

18. The United States Government has exclusive sovereignty over airspace of the United States pursuant to 49 U.S.C.A. § 40103. The airspace, therefore, is not subject to private ownership nor can the flight of an aircraft within the navigable airspace of the United States constitute a trespass. Unmanned aircraft are aircraft consistent with Subtitle B of Public Law

83

112-95 and the existing definition of aircraft in Title 49 of the United States Code, 49 U.S.C. 40102.

19. In addition, even if Plaintiff had viewed the defendant's property from the air, which he did not, such viewing would not violate the defendant's reasonable expectation of privacy according to well established federal law. The U.S. Supreme Court has determined, as a general rule, that there is no reasonable expectation of privacy in the area surrounding a home in plain view from above. *California v. Ciraolo,* 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986); *Florida v. Riley,* 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989) (plurality opinion). Resolution of the current dispute between Plaintiff and Defendant requires the application of this existing federal case law to an as yet unexamined technology – unmanned aircraft.

20. Further, Congress has indicated its unambiguous intent to ensure the safety of aircraft. Pursuant to 18 U.S.C.A. § 32, whoever "sets fire to, damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States or any civil aircraft used, operated, or employed in interstate, overseas, or foreign air commerce" commits a felony. Although this statute may not create a private right of action, the interpretation of the statute is critical to the determination of the claims asserted herein. Should the court determine that this statute applies to unmanned aircraft, as it should, that would leave no room for Defendant's assertion of the right to self-help or the Kentucky District Court Judge's ruling that Defendant was "within his rights" to shoot the aircraft.

21. Conversely, Kentucky law regarding trespass does not specifically address the rights of unmanned aircraft to traverse the skies above private property. It defines a trespasser as "any person who enters or goes upon the real estate of another without any right, lawful authority

84

or invitation, either expressed or implied." Ky. Rev. Stat. Ann. § 381.231. A trespasser may be subject to civil suit and/or criminal prosecution. Kentucky law also permits resort to self-help in response to trespass. A landowner may use physical force "upon another person when the person believes that such force is immediately necessary to prevent the commission of criminal trespass." Ky. Rev. Stat. Ann. § 503.080.

22. Given the clear conflict of federal and state laws, as applied to the facts of this action, Plaintiff desires a judicial determination of the respective rights and duties of Plaintiff and Defendant with respect to Plaintiff's rights to operate an aircraft within Class G airspace and recover damages for trespass to chattel caused by Defendant's intentional shooting of that aircraft.

23. Plaintiff is, herein, asserting a claim for trespass to chattels as a result of the damages to his aircraft.

24. The ruling of the Kentucky District Court and assertions made by Defendant regarding his belief that his actions were justified because Plaintiff was engaged in trespass and invasion of privacy are in direct conflict with established federal law governing the regulation of manned aircraft and airways and cannot be resolved without addressing how this law applies to unmanned aircraft

25. For those reasons, Plaintiff seeks the following declaratory judgment:

(A) An unmanned aircraft is an "aircraft" according to Federal law.

(B) An unmanned aircraft operating in Class G airspace in the manner alleged above is operating in "navigable airspace" within the exclusive jurisdiction of the United States.

(C) That Plaintiff was operating his unmanned aircraft in the navigable airspace within the exclusive jurisdiction of the United States and not within Defendant's property;

85

(D) That the operation of his unmanned aircraft in in the manner alleged above did not violate the defendant's reasonable expectation of privacy; and

(E) That a property owner cannot shoot at an unmanned aircraft operating in navigable airspace within the exclusive jurisdiction of the United States when that aircraft is operating in the manner alleged above.

SECOND CLAIM FOR RELIEF
(Trespass to Chattels)

26. Plaintiff incorporates by reference the allegations in the foregoing paragraphs as though fully set forth.

27. Defendant intentionally intermeddled with personal property in the possession of Plaintiff, specifically, his unmanned aircraft.

28. Defendant impaired the property as to its condition, quality, to value.

29. Plaintiff's property was damaged by the reduced value, condition and quality of his aircraft in an amount of approximately $1,500.00.

WHEREFORE, premises considered, Plaintiff demands the following relief:

1. That the Defendant be served with process and answer the allegations and claims set forth above;

2. That the court enter the declaratory judgment requested in the First Cause of Action, above; and

3. That the Court award to the Plaintiff such other legal and equitable relief as it deems appropriate, including monetary damages, prejudgment interest, and the costs of filing this action.

86

Respectfully submitted,

s/ Thomas C. Gleason
Thomas C. Gleason
FROST BROWN TODD LLC
400 West Market Street, 32nd Floor
Louisville, KY 40202
(502) 589-5400
(502) 581-1087 fax
tgleason@fbtlaw.com

s/ James E. Mackler
James E. Mackler *(pro hac vice pending)*
William L. Campbell, Jr. *(pro hac vice pending)*
FROST BROWN TODD LLC
150 3rd Ave. S., Suite 1900
Nashville, TN 37201
(615) 251-5550
jmackler@fbtlaw.com
ccampbell@fbtlaw.com

Attorneys for Plaintiff

87

California Prepares New Drone Laws

Two California lawmakers have introduced two separate bills this week that would further regulate drones in America's most populous state. If passed, one of the new state laws would require "tiny physical or electronic license plates" and inexpensive insurance, among other requirements. A second bill would compel drone pilots who are involved in incidents that damage property or injure people to leave their contact information—similar to what drivers must do following auto accidents.

The proposed laws are in response to a series of unfortunate mishaps involving drones across the Golden State in 2015: there were some unmanned aerial vehicles that got in the way of fire-fighting efforts, while another crashed into power lines in Hollywood, and yet another hit a baby in Pasadena.

The first bill, which was authored by Assemblyman Mike Gatto (D-Glendale), would require drone pilots to hold "inexpensive ($1, or so) insurance policies sold at the point-of-sale"—a press release compared it to automobile insurance.

Gatto's bill, which has yet to be formally introduced with actual legislative text in the state assembly, would also require that all GPS-enabled drones "of a certain size" have an "automatic shut-off technology that would activate if approaching an airport."

"I think 2015 showed us that in the era of democratized aviation, certain types of incidents will be fairly common," he told Ars. "More and more people are buying these and that's great. This is just like the 1920s when more and more people were buying cars, but I just think that we need some basic rules going forward."

88

He expects the bill to be introduced next week.The second bill, written by Assembly member Ed Chau (D-Monterey Park), aims to counter "hit and run" drone accidents by ordering drone pilots to leave their identifying information in a conspicuous place at the scene of the accident."Unfortunately, as the number of drones in the air will only increase in the coming years, we are going to see more and more accidents," Chau said in a statement. "And even with world-class safety features and training, accidents are still going to happen, just like on our roadways. If a drone breaks down, runs out of power or crashes into something, the operator needs to do the responsible thing and come forward and identify himself to the victim and to the police. This bill will make that responsibility the law."

Golden State of Mind

Amanda Essex, a policy analyst with the National Conference of State Legislatures, told Ars that Chau's drone bill was unique amongst similar state laws.

"A few states have considered legislation related to unmanned aircraft systems (UAS) registration or insurance requirements, both of which are included in Assembly member Gatto's legislation," she told Ars by e-mail. "Legislation has not yet been enacted in any state that I am aware of requiring registration or insurance for non-commercial UAS. Geo-fencing, another provision of Assemblymember Gatto's bill, has also been introduced in other states, including New Jersey."

The drone industry has yet to respond to these new bills.

"We're still reviewing this legislation in California and other bills across the rest of the country that were recently introduced with the start of the state legislative sessions," Tom McMahon, a vice president of the Association of Unmanned Vehicle Systems International, a drone trade group, told Ars. "We currently don't have positions on these bills."

Brendan Schulman, lawyer for drone maker DJI, did not immediately respond to Ars' request for comment.

Gatto was confident that California's regulations could have an outsized influence on drones sold nationwide.

"California has a long history of leading the way with sensible requirements for certain products sold in the state of California," he said. "In 1971, California was the only jurisdiction in the country that cars had smog control devices—now, all 50 states require catalytic converters."

89

The bills would have to pass both the state assembly and the state senate, and they would need to be signed by Gov. Jerry Brown (D), who vetoed a bill in September 2015 that would have banned drone flights over private property at 350 feet or below.

Source: ars technica

Download article as PDF

Posted in Regulatory Matters on January 19, 2016 by The Editor. Leave a comment

← GENERAL ATOMICS GETS $57M LOGISTICS CONTRACT FOR UK SAAB TO DELIVER UAS TO SWEDISH POLICE →

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

90

AB-1662 Unmanned aircraft systems: accident reporting. (2015-2016)

CALIFORNIA LEGISLATURE— 2015–2016 REGULAR SESSION

ASSEMBLY BILL **No. 1662**

Introduced by Assembly Member Chau

January 13, 2016

An act to add Section 20019 to the Vehicle Code, relating to unmanned aircraft systems.

LEGISLATIVE COUNSEL'S DIGEST

AB 1662, as introduced, Chau. Unmanned aircraft systems: accident reporting.

Existing federal law, the Federal Aviation Administration Modernization and Reform Act of 2012, provides for the integration of unmanned aircraft systems, commonly known as drones, into the national airspace system. Existing federal law requires the operator of an unmanned aircraft system to immediately, and by the most expeditious means available, notify the nearest National Transportation Safety Board office when, among other things, an aircraft accident, as defined, or certain serious incidents occur. Those notifications are required to include, among other things, the name of the owner of the unmanned aircraft system, the name of the operator of the unmanned aircraft system, the date and time of the accident, and the nature of the accident.

Existing state law requires the driver of a vehicle involved in an accident resulting in injury to any person, other than himself or herself, or in the death of any person, to immediately stop the vehicle at the scene of the accident and provide certain information and render assistance, as necessary, to the driver and occupants of the other vehicle and provide the specified information to any traffic or police officer at the scene of the accident. A person who violates this requirement is guilty of a misdemeanor or a felony. Existing law requires the driver of a vehicle involved in an accident resulting only in damage to any property, including vehicles, to immediately stop the vehicle at the nearest location that will not impede traffic or otherwise jeopardize the safety of other motorists and provide certain information to the owner or person in charge of the damaged property or place that information in a conspicuous place on the damaged property. A person who violates this requirement is guilty of a misdemeanor.

This bill would require the operator of any unmanned aircraft system involved in an accident resulting in injury to an individual or damage to property to immediately land the unmanned aircraft at the nearest location that will not jeopardize the safety of others and provide certain information to the injured individual or the owner or person in charge of the damaged property or place that information in a conspicuous place on the damaged property. The bill would make a person who violates these provisions guilty of a misdemeanor. By creating a new crime, the bill would impose a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

91

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: yes

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Section 20019 is added to the Vehicle Code, to read:

20019. (a) The operator of any unmanned aircraft system involved in an accident resulting in injury to an individual or damage to property shall immediately land the unmanned aircraft at the nearest location that will not jeopardize the safety of others. Moving the unmanned aircraft in accordance with this subdivision does not affect the question of fault. The operator shall also immediately do one of the following:

(1) Present his or her valid identification, if he or she has that identification, and his or her name and current residence address to the injured individual. For purposes of this section, "valid identification" includes, but is not limited to, a driver's license, a state-issued identification card, or a passport.

(2) Locate and notify the owner or person in charge of that property of the name and address of the operator of the unmanned aircraft system involved and, upon locating the owner or person in charge of the damaged property and being requested to do so, present his or her valid identification, if he or she has that identification, and his or her name and current residence address to the other property owner or person in charge of the damaged property.

(3) Leave in a conspicuous place on the damaged property a written notice giving the name and address of the operator of the unmanned aircraft system involved and a statement of the circumstances of the accident and, without unnecessary delay, notify the police department of the city where the damage occurred or, if the damage occurred in unincorporated territory, the local headquarters of the sheriff's department of the county where the damage occurred.

(b) Except as provided in subdivision (c), a person who fails to comply with the requirements of this section is guilty of a misdemeanor, punishable by imprisonment in the county jail not exceeding six months, or by a fine not exceeding one thousand dollars ($1,000), or by both that imprisonment and fine.

(c) This section does not apply to either of the following:

(1) A law enforcement officer, or an employee of a police department or other law enforcement agency, operating an unmanned aircraft system within the scope of his or her employment.

(2) A person operating an unmanned aircraft system pursuant to the specific authorization of the Federal Aviation Administration if the person operates the unmanned aircraft system in accordance with the terms and conditions of that authorization.

(d) For purposes of this section, the following definitions apply:

(1) "Unmanned aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

(2) "Unmanned aircraft system" means an unmanned aircraft and associated elements, including, but not limited to, communication links and the components that control the unmanned aircraft that are required for the pilot in command to operate safely and efficiently in the national airspace system.

SEC. 2. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

92