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

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 E. 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

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.

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*.