Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

Consensus, Stakeholder-Drafted
Best Practices Created
in the NTIA-Convened
Multistakeholder Process

May 18, 2016

"Unmanned Aircraft Systems (UAS) technology continues to improve rapidly, and increasingly UAS are able to perform a variety of missions with greater operational flexibility and at a lower cost than comparable manned aircraft. …

–President Barack Obama

Charge from the President

As compared to manned aircraft, UAS may provide lower-cost operation and augment existing capabilities while reducing risks to human life. Estimates suggest the positive economic impact to U.S. industry of the integration of UAS into the NAS could be substantial and likely will grow for the foreseeable future.

The combination of greater operational flexibility, lower capital requirements, and lower operating costs could allow UAS to be a transformative technology in the commercial and private sectors for fields as diverse as urban infrastructure management, farming, and disaster response. Although these opportunities will enhance American economic competitiveness, our Nation must be mindful of the potential implications for privacy, civil rights, and civil liberties. The Federal Government is committed to promoting the responsible use of this technology in a way that does not diminish rights and freedoms.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to establish transparent principles that … promote the responsible use of this technology in the private and commercial sectors, it is hereby ordered as follows: …

There is hereby established a multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the NAS. The process will include stakeholders from the private sector. Within 90 days of the date of this memorandum, the Department of Commerce, through the National Telecommunications and Information Administration, and in consultation with other interested agencies, will initiate this multi-stakeholder engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use."

President Barack Obama
FEBRUARY 15, 2015

Consensus, Stakeholder-Drafted Best Practices
Created in the NTIA-Convened Multistakeholder Process

I. Introduction

The benefits of commercial and private unmanned aircraft systems (UAS) are substantial. Technology has moved forward rapidly, and what used to be considered toys are quickly becoming powerful commercial tools that can provide enormous benefits in terms of safety and efficiency. UAS integration will have a significant positive economic impact in the United States. Whether UAS are performing search and rescue missions, allowing farmers to be more efficient and environmentally friendly, inspecting power lines and cell towers, gathering news and enhancing the public's access to information, performing aerial photography to sell real estate and provide insurance services, surveying and mapping areas for public policy, delivering medicine to rural locations, providing wireless internet, enhancing construction site safety, or more—society is only just beginning to realize the full potential of UAS. UAS technology is already bringing substantial benefits to people's daily lives, including cheaper goods, innovative services, safer infrastructure, recreational uses, and greater economic activity. Inevitably, creative minds will devise many more UAS uses that will save lives, save money and make our society more productive.

However, the very characteristics that make UAS so promising for commercial and non-commercial uses, including their small size, maneuverability and capacity to carry various kinds of recording or sensory devices, can raise privacy concerns. As a result, individuals may be apprehensive about the adoption of this technology into everyday life. In order to ensure that UAS and the exciting possibilities that come with them live up to their full potential, operators should use this technology in a responsible, ethical, and respectful way. This should include a commitment to transparency, privacy and accountability.

The purpose of this document is to outline and describe voluntary Best Practices that UAS operators could take to advance UAS privacy, transparency and accountability for the private and commercial use of UAS.[1] UAS operators may implement these Best Practices in a variety of ways, depending on their circumstances and technology uses, and evolving privacy expectations. In some cases, these Best Practices are meant to go beyond existing law and they do not—and are not meant to—create a legal standard of care by which the activities of any particular UAS operator should be judged. These Best Practices are also not intended to serve as a template for future statutory or regulatory obligations, in part because doing so would make these standards mandatory (not voluntary) and could therefore raise First Amendment concerns.

1 The National Telecommunications and Information Administration (NTIA) has convened a series of multi-stakeholder efforts as a way to increase privacy protections based upon the Administration's framework for consumer information privacy. On February 15, 2015, President Obama issued a Presidential Memorandum instructing NTIA to convene such a process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the National Airspace System. These Voluntary Best Practices are the result of that multi-stakeholder engagement process.

II. Applicability

These voluntary Best Practices for UAS focus on data collected via a UAS, which includes both commercial and non-commercial UAS. The only section applicable to newsgatherers and news reporting organizations is Section V considering that their activity is strongly protected by the First Amendment to the Constitution of the United States. There is also an Appendix entitled, "Guidelines for Neighborly Drone Use" that is intended to be a quick and easy reference guide for recreational UAS operators.

These Best Practices do not apply to data collected by other means—for instance, a company need not apply these Best Practices to data collected via the company's website. These Best Practices do not apply to the use of UAS for purposes of emergency response, including safety and rescue responses.

Nothing in these Best Practices shall:

- Be construed to limit or diminish freedoms guaranteed under the Constitution;
- Replace or take precedence over any local, state, or federal law or regulation;
- Take precedence over contractual obligations or the representations of entities contracting UAS operators. However, entities contracting UAS operators should consider these Best Practices when setting the terms of a contract for UAS use, and UAS operators should consider these Best Practices when choosing to accept a contract for UAS use; or
- Impede the safe operation of a UAS.

UAS operators should comply with all applicable laws and regulations. These Best Practices are intended to encourage positive conduct that complements legal compliance. Operators who are aware of other best practices that may apply specific guidance to technologies deployed on or through UAS should consider how to incorporate that guidance into their privacy and security policies and practices.

These Best Practices are also not intended to serve as a template for future statutory or regulatory obligations, in part because doing so would raise First Amendment issues.

III. Definitions

The term "*consent*" means words or conduct indicating permission. Consent must be informed and conduct indicating permission may be express or implied, depending on the context.

"Covered data" means information collected by a UAS that identifies a particular person. If data collected by UAS likely will not be linked to an individual's name or other personally identifiable information, or if the data is altered so that a specific person is not recognizable, it is not covered data.

The term "*data subjects*" refers to the individuals about whom covered data is collected.

The terms *"where practicable"* and "*reasonable*" depend largely on the circumstances of the UAS operator, the sensitivity of data collected, and the context associated with a particular UAS operation.

IV. Voluntary Best Practices

These voluntary Best Practices for UAS focus on data collected via a UAS, which includes both commercial and non-commercial UAS. The only section applicable to newsgatherers and news reporting organizations is Section V considering that their activity is strongly protected by the First Amendment to the Constitution of the United States. There is also an Appendix entitled, "Guidelines for Neighborly Drone Use" that is intended to be a quick and easy reference guide for recreational UAS operators.

These Best Practices do not apply to data collected by other means—for instance, a company need not apply these Best Practices to data collected via the company's website. These Best Practices do not apply to the use of UAS for purposes of emergency response, including safety and rescue responses.

1. Inform Others of Your Use of UAS

1(a) Where practicable, UAS operators should make a reasonable effort to provide prior notice to individuals of the gener-al timeframe and area that they may anticipate a UAS inten-tionally collecting covered data.[2]

1(b) When a UAS operator anticipates that UAS use may result in collection of covered data, the operator should provide a privacy policy for such data appropriate to the size and complexity of the operator, or incorporate such a policy into an existing privacy policy. The privacy policy should be in place no later than the time of collection and made publicly available. The policy should include, as practicable:

(1) the purposes for which UAS will collect covered data;[3]

(2) the kinds of covered data UAS will collect;

(3) information regarding any data retention and de-identification practices;[4]

(4) examples of the types of any entities with whom covered data will be shared;

(5) information on how to submit privacy and security complaints or concerns; and

(6) information describing practices in responding to law enforcement requests.

Material changes to the above should be incorporated into the privacy policy.

2. Show Care When Operating UAS or Collecting and Storing Covered Data

2(a) In the absence of a compelling need to do otherwise, or consent of the data subjects, UAS operators should avoid

2 What qualifies as a practicable and reasonable effort to provide prior notice will depend on operators' circumstances and the context of the UAS operation. For example, delivery UAS operators may provide customers with an estimated time of delivery. Real estate professionals using UAS may provide a home seller (and possibly immediate neighbors) with prior notice of the estimated date of UAS photography of the property. Hobbyist UAS operators may not need to notify nearby individuals of UAS flight in the vicinity.

3 These Best Practices recognize that UAS operators may not be able to predict all future uses of data. Accordingly, these Best Practices do not intend to discourage unplanned or innovative data uses that may result in desirable economic or societal benefits.

4 If it is not practicable to provide an exact retention period, because, for example, the retention period depends on legal hold requirements or evolving business operations, the UAS operator may explain that to data subjects when disclosing its retention policies.

using UAS for the specific purpose of intentionally collecting cov-ered data where the operator knows the data subject has a reasonable expectation of privacy.

2(b) In the absence of a compelling need to do otherwise, or consent of the data subjects, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of covered data about individuals.

2(c) Where it will not impede the purpose for which the UAS is used or conflict with FAA guidelines, UAS operators should make a reasonable effort to minimize UAS operations over or within private property without consent of the property owner or without appropriate legal authority.

2(d) UAS operators should make a reasonable effort to avoid knowingly retaining covered data longer than reasonably necessary to fulfill a purpose as outlined in § IV.1(b). With the consent of the data subject, or in exceptional circumstances (such as legal disputes or safety incidents), such data may be held for a longer period.

2(e) UAS operators should establish a process, appropriate to the size and complexity of the operator, for receiving privacy or security concerns, including requests to delete, de-identi-fy, or obfuscate the data subject's covered data. Commercial operators should make this process easily accessible to the public, such as by placing points of contact on a company website.[5]

3. Limit the Use and Sharing of Covered Data

3(a) UAS operators should not use covered data for the following purposes without consent: employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligi-bility other than when expressly permitted by and subject to the requirements of a sector-specific regulatory framework.

3(b) UAS operators should make a reasonable effort to avoid using or sharing covered data for any purpose that is not included in the privacy policy covering UAS data.

3(c) If publicly disclosing covered data is not necessary to ful-fill the purpose for which the UAS is used, UAS operators should avoid knowingly publicly disclosing data collected via UAS until the operator has undertaken a reasonable effort to obfuscate or de-identify covered data —unless the data subjects provide consent to the disclosure.

3(d) UAS operators should make a reasonable effort to avoid us-ing or sharing covered data for marketing purposes unless the data subject provides consent to the use or disclosure. There is no restriction on the use or sharing of aggregat-ed covered data as an input (e.g., statistical information) for broader marketing campaigns.

4. Secure Covered Data

4(a) UAS operators should take measures to manage security risks of covered data by implementing a program that contains reasonable administrative, technical, and physical safe-guards appropriate to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the covered data.

Examples of appropriate administrative, technical, and physical safeguards include those described in guidance from the Federal Trade Commission, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the Interna-tional Organization for Standardization's 27001 standard for in-formation security management.

For example, UAS operators engaging in commercial activity should consider taking the following actions to secure covered data:

- Having a written security policy with respect to the collection, use, storage, and dissemination of covered data appropriate to the size and complexity of the operator and the sensitivity of the data collected and retained.[6]
- Making a reasonable effort to regularly monitor systems for breach and data security risks.
- Making a reasonable effort to provide security training to employees with access to covered data.
- Making a reasonable effort to permit only authorized individuals to access covered data.

5. Monitor and Comply with Evolving Federal, State, and Local UAS Laws

5(a) UAS operators should ensure compliance with evolving applicable laws and regulations and UAS operators' own privacy and security policies through appropriate internal processes.

5 This may be as simple as talking to an individual who approaches the UAS operator with a concern.

6 As with the privacy policy referenced in § IV.1(b), UAS operators may modify a broader existing security policy to incorporate data collected via UAS. A security policy should include, at minimum, such basic steps as keeping software up to date and downloading security patches for known vulnerabilities.

V. Best Practices for Newsgatherers and News Reporting Organizations

Newsgathering and news reporting are strongly protected by United States law, including the First Amendment to the Constitution. The public relies on an independent press to gather and report the news and ensure an informed public.

For this reason, these Best Practices do not apply to newsgatherers and news reporting organizations. Newsgatherers and news reporting organizations may use UAS in the same manner as any other comparable technology to capture, store, retain and use data or images in public spaces. Newsgatherers and news reporting organizations should operate under the ethics rules and standards of their organization, and according to existing federal and state laws.

Appendix

Guidelines for Neighborly Drone Use

Drones are useful. New, fairly cheap drones are easy to use. But just because they are cheap and simple to fly doesn't mean the pictures and video they take can't harm other people. The FAA and partner organizations have put safety guidance online at **http://knowbeforeyoufly.org**. But even safe flight might not respect other people's privacy. These are voluntary guidelines. No one is forcing you to obey them. Privacy is hard to define, but it is important. There is a balance between your rights as a drone user and other people's rights to privacy. That balance isn't easy to find. You should follow the detailed "UAS Privacy Best Practices", on which these guidelines are based, especially if you fly drones often, or use them commercially. The overarching principle should be peaceful issue resolution.

1. If you can, tell other people you'll be taking pictures or video of them before you do.
2. If you think someone has a reasonable expectation of privacy, don't violate that privacy by taking pictures, video, or otherwise gathering sensitive data, unless you've got a very good reason.
3. Don't fly over other people's private property without permission if you can easily avoid doing so.
4. Don't gather personal data for no reason, and don't keep it for longer than you think you have to.
5. If you keep sensitive data about other people, secure it against loss or theft.
6. If someone asks you to delete personal data about him or her that you've gathered, do so, unless you've got a good reason not to.
7. If anyone raises privacy, security, or safety concerns with you, try and listen to what they have to say, as long as they're polite and reasonable about it.
8. Don't harass people with your drone.

Supporters

As of June 2016

Amazon

Association for Unmanned Vehicle Systems International (AUVSI)

Center for Democracy and Technology

Commercial Drone Alliance

Consumer Technology Association

CTIA

Digital Content Next (DCN)

Future of Privacy Forum

Intel

National Association of Broadcasters (NAB)

New America's Open Technology Institute

News Media Coalition

Newspaper Association of America (NAA)

NetChoice

Online Trust Alliance (OTA)

PrecisionHawk

Radio Television Digital News Association (RTDNA)

Small UAV Coalition

Software & Information Industry Association (SIIA)

U.S. Chamber of Commerce

X (Formerly Google [x])

To add your organization to the list of supporters, please email drones@fpf.org

"As the President recognized when he directed NTIA to convene this process, these best practices can help promote Commerce priorities by allowing the industry to grow, develop and innovate while helping to build consumer trust."

– U.S. Secretary of Commerce Penny Pritzker

"The best practices agreed to by a diverse group of stakeholders—including privacy and consumer advocates, industry, news organizations and trade associations—represent an important step in building consumer trust, giving users the tools to innovate in this space in a manner that respects privacy, and providing accountability and transparency."

– NTIA Deputy Assistant Secretary Angela Simpson

The best practices were developed by a group of stakeholders convened by the National Telecommunications and Information Administration.
This is not a government publication.

More information about the NTIA process is available at **www.ntia.doc.gov**.
An easy to read summary of the best practices is available at **www.fpf.org**