Ballard Spahr LLP

1909 K Street, NW
12th Floor
Washington, DC 20006-1157
TEL 202.661.2200
FAX 202.661.2299
www.ballardspahr.com

Charles D. Tobin
202.661.2218
tobinc@ballardspahr.com

August 2, 2022

Via E-mail (9-FAA-UAS-BVLOS@faa.gov)

Federal Aviation Administration
BVLOS Aviation Rulemaking Committee

Re: Privacy and the UAS BVLOS Aviation Rulemaking Committee Final Report

Introduction

We write today on behalf of the News Media Coalition ("Coalition"), which consists of news media organizations with a significant interest in the development of drone law and policy in the United States.[1] We appreciate the two recent virtual listening opportunities that the FAA livestreamed to receive comments concerning the work of the Unmanned Aircraft Systems Beyond Visual Line of Sight Aviation Rulemaking Committee and its Final Report ("Final Report").

We write to supplement the record of the virtual listening opportunities with the Coalition's concern about the discussion of the issue of privacy contained in the BVLOS ARC's Final Report.

The Coalition participated in earnest throughout the FAA ARC process, and as reflected in the comments we previously submitted with the Final Report (attached as Exhibit A), we concurred in the language of the Final Report, with one small but significant exception. As we stated, the Coalition does not agree with the phrase in the Final Report that, within the BVLOS ARC, there was "general consensus that further consideration should be given to statutory privacy protections." Final Report, 60:1934-35. As we noted in our previous comments, the Coalition's concerns with this language are three-fold: (1) there was not, in fact, "consensus" that statutory, drone-specific privacy protections warranted further consideration among the stakeholders participating in the ARC, (2) the Coalition disagrees that the BVLOS rulemaking process gives rise to an occasion for Congress to create new "statutory privacy protections", and (3) the FAA has already determined, appropriately, that its mission does not include the development of new privacy laws or regulations. *See* Ex. A.

[1] A complete list of Coalition members may be found on page 4.

Today we write to reinforce these concerns. During the Coalition's participation in the ARC, and in our review of comments submitted by our fellow ARC committee members, just three organizations out of the dozens of participants advocated for consideration of new statutory privacy protections specifically targeting drone operations.[2] At no time in that process did these organizations present their proposals to the full ARC membership, nor did the ARC reach a consensus to include in the Final Report any recommendation that the FAA consider new privacy regulations or statutory regimes.

Indeed, during Phase 1 of the ARC, ARC leadership established a Privacy and Data Sharing Task Group to weigh privacy concerns and to develop any recommendations for Phase 2. Our Coalition and the Electronic Frontier Founder led the Privacy and Data Sharing Task Group, and together we generated a report, approved by the Phase 1 ARC Security Subgroup and incorporated into the Phase 1 draft final report seven months before the ARC completed its Final Report. We attach (as Exhibit B) the BVLOS ARC Privacy and Data Sharing Task Group Report.

As the Privacy and Data Sharing Task Group's report recognized, BVLOS operations can implicate the privacy interests of different stakeholder groups, including UAS operators, UAS customers and the general public. The Task Group recognized that "not all types of operations pose the same level of security risks," and that any BVLOS regulation should "account for these varying degrees of security and privacy concerns." Ex. B at 2. And notably, the Privacy and Data Sharing Task Group made clear—in contrast to the ARC's Final report—that the FAA should "[r]efrain from writing privacy laws" and that the BVLOS rulemaking process would not warrant the FAA's reconsideration of its past determination "that the privacy of the general public was out of scope" of its UAS rulemaking authority, including during the rulemaking proceedings related to Part 107, Remote ID and Surveillance, and Flight Operations Over People. Ex. B at 3 (emphasis added). Instead, the Task Group agreed that "this process is not suited for drafting comprehensive privacy laws." *Id*. In other words, not only was there no consensus to revisit privacy laws during the BVLOS ARC process, but the consensus of the Task Group was to not revisit those issues.[3]

[2] The Electronic Frontier Foundation (EFF), the Electronic Privacy Information Center (EPIC), and the American Civil Liberties Union (ACLU).

[3] As the Coalition highlighted in its concurring comments to the BVLOS Final Report, however, a robust set of technology-neutral state privacy statutes and common law already protects against unlawful use of recording devices in private spaces, balancing the American public's interest in a free and open society with the legitimate privacy interests of the larger community. See Exhibit A at 6, n. 6-7. New privacy laws specifically targeting drone

The FAA previously recognized, in promulgating Part 107, that the types of privacy issues raised and rejected in the BVLOS ARC deliberations are outside of the FAA's scope. *See* Final Rule, *Operation and Certification of Small Unmanned Aircraft Systems*, 81 Fed. Reg. 42064, 42190 (June 28, 2016). For this reason, in examining the implication of data management issues with the emerging drone industry, the White House – rather than calling on Congress to legislate new privacy codes, or the FAA to develop new privacy regulation – delegated the discussion to a voluntary multistakeholder process facilitated by the National Telecommunications and Information Administration. That body deliberated for more than a year and promulgated a set of voluntary best practices, explicitly noting that the best practices were "not intended to serve as a template for future statutory or regulatory obligations, in part because doing so would raise First Amendment issues."[4] Indeed, given the important First Amendment implications for news organizations, and even though the best practices document is strictly voluntary, the participants adopted an explicit carve-out for newsgathering activity:

> 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.

Ex. C at 7.

In conformity with the White House and FAA's long recognition that the FAA's mission and expertise do not include privacy issues, the BVLOS ARC participants refrained from considering whether to suggest the consideration of any new privacy regulation. The last-minute addition to the Final Report language does not accurately reflect the lengthy ARC discussions, the recommendation of the ARC's Privacy and Data Sharing Task Force, and the White House and FAA's wise determination to leave that issue to the robust body of existing privacy laws.[5] The Coalition therefore disagrees with the phrase in the BVLOS

---

operations are therefore not necessary and would instead needlessly provoke endless confrontation over constitutional issues.

[4] *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*, NTIA, May 18, 2016 (attached as Ex. C).

[5] Moreover, the organizations pressing for more burdensome, drone-specific privacy laws proposed to the ARC a specific regime that would, perhaps unintentionally though unavoidably, threaten the safety, in addition to the First Amendment rights, of journalists and those operating drones in furthering their political speech by permitting the government and the public to identify the operator and mission for every BVLOS operation.

ARC Final Report that there was "general consensus that further consideration should be given to statutory privacy protections."

The opportunities afforded by BVLOS operations are many, and the promise of enhanced newsgathering operations are no exception. The Coalition thanks the FAA and ARC leadership for their continued attention to this matter and stands ready to demonstrate that BVLOS operations can serve communities in a safe, positive manner.

Sincerely,

Charles D. Tobin, Ballard Spahr LLP
Emmy Parsons, Ballard Spahr LLP
Joel Roberson, Holland & Knight LLP

On behalf of the News Media Coalition:

Advance/Newhouse Partnership
American Broadcasting Companies, Inc.
The Associated Press
Capitol Broadcasting Co.
Fusion Media Network
Gannett Co., Inc.
Getty Images (US), Inc.
National Press Photographers Association
NBCUniversal Media, LLC
News Media Alliance
The New York Times Company
The E.W. Scripps Company
Sinclair Broadcast Group, Inc.
TEGNA, Inc.
WP Company LLC

Exhibit A

Ballard Spahr LLP

1909 K Street, NW
12th Floor
Washington, DC 20006-1157
TEL 202.661.2200
FAX 202.661.2299
www.ballardspahr.com

Charles D. Tobin
Tel: 202.661.2218
Fax: 202.661.2299
tobinc@ballardspahr.com

March 3, 2022

Federal Aviation Administration
BVLOS Aviation Rulemaking Committee

Re: The News Media Coalition's Statement of Concurrence with One Exception Regarding the UAS BVLOS Aviation Rulemaking Committee Final Report

Introduction

The News Media Coalition ("Coalition"), consisting of news media organizations with significant interest in the development of drone law and policy in the United States, submits these comments on behalf of news executives, journalists, viewers, readers, and social media users regarding the Unmanned Aircraft Systems Beyond Visual Line of Sight Aviation Rulemaking Committee's Final Report ("Final Report").

The Coalition appreciates the opportunity to participate in the FAA ARC process. The Coalition concurs in the Final Report, with the exception of one phrase. We do not agree with the language of the Final Report that recites that there was "general consensus that further consideration should be given to statutory privacy protections." Final Report, 60:1934-35. The Coalition's concerns with this language are three-fold: (1) there was not, in fact, "consensus" on this issue among the stakeholders participating in the ARC, (2) the Coalition does not believe that the BVLOS rulemaking process gives rise to an occasion for Congress to create new "statutory privacy protections", and (3) the FAA has already determined, appropriately, that its mission does not include the development of new privacy laws or regulations.

The News Media Coalition[1] consists of:

- The nation's leading television and cable networks;
- The leading national newspapers;
- More than 479 television stations serving local U.S. markets;

[1] The members of the Coalition are listed on page 10.

- More than 545 regional and local U.S. newspapers;
- More than 35 U.S. radio stations;
- More than 570 local market websites;
- Content providers for hundreds of online and mobile platforms and devices;
- The leading wire services in the U.S. and abroad;
- The largest stock film and photo agencies worldwide;
- The leading professional association of visual journalists;
- The country's premier trade association representing independent photographers; and
- The leading membership association for content providers in all media, supported by more than 115 media members and 200 law firms worldwide.

The companies that make up the Coalition represent a wide cross-section of the news professionals who provide Americans each day with the news they need. They also represent one of the sectors of the economy that is most engaged with the development of sound regulations and best practices governing Unmanned Aircraft Systems ("UAS" or "drones"). While the member companies compete in markets across the country, they have come together in the unified belief that preserving the right to gather news, including by drones, is not a competitive issue but one of universal, and great, importance.

For the past several years, the Coalition has worked cooperatively with the federal government toward the development of statutes, regulations, industry training, and professional best practices for the safe gathering of news by drones. At the same time, the Coalition has strongly encouraged the maintenance of the existing legal framework for privacy protection, especially as it concerns the ability to gather news and information for the public benefit. As part of those efforts, the Coalition actively participated in the rulemaking process that led to the June 2016 implementation of 14 C.F.R. Part 107. In addition, the Coalition has engaged in efforts to integrate the use of drones by journalists into the national airspace system ("NAS"), including:

- Partnering with Virginia Tech through the Mid-Atlantic Aviation Partnership, one of six FAA-designated test sites, to collect data and evaluate the safe use of UAS by journalists for newsgathering (2015);
- Submitting public comments in response to the FAA's NPRM on the "Operation and Certification of Small Unmanned Aircraft Systems" (April 2015);
- Serving as an appointed member on the FAA Micro Unmanned Aircraft Systems Aviation Rulemaking Committee (April 2016);
- Participating in the National Telecommunications and Information Administration (NTIA) multi-stakeholder process on drone privacy, which

culminated in a set of sensible, voluntary "best practices" that exempted First Amendment protected newsgathering (May 2016);
- Submitting public comments to the Federal Trade Commission Fall Seminar Series on Emerging Consumer Technology Issues: Drones (October 2016);
- Participating in the FAA Unmanned Aircraft Safety Team;
- Submitting public comments in response to the FAA's NPRM on the "Operation of Small Unmanned Aircraft Systems Over People" (April 2019);
- Submitting public comments in response to the FAA's NPRM on the "Safe and Secure Operations of Small Unmanned Aircraft Systems" (April 2019); and
- Submitting public comments in response to the FAA's NPRM on the "Remote Identification of Unmanned Aircraft Systems" (March 2020)

In addition, the Coalition served as an appointed member of the FAA's UAS Identification and Tracking Aviation Rulemaking Committee ("UAS-ID ARC"). The UAS-ID ARC included members from federal, state and local governments, law enforcement, drone manufacturers, drone software developers, and drone operators, including journalists. The Coalition provided input on the development of the FAA rulemaking to establish a drone remote identification standard that ensures safety and security of the NAS, while protecting journalists' First Amendment right to newsgathering. In September 2017, at the conclusion of the UAS-ID ARC, the Coalition filed a dissent to the ARC's final report insisting on greater First Amendment protections and less burdensome notification and recordkeeping requirements.[2]

Overview of the Coalition's Comments

The Coalition disagrees that there was "general consensus" among ARC membership that the FAA should consider statutory privacy protections, and for the reasons outlined below, the Coalition firmly believes that the current legal and statutory environment appropriately balances the privacy interests of individuals against the First Amendment rights of journalists to gather and disseminate news. The FAA's proposed rulemaking should, rather than propose a new privacy statutory regime, continue to foster an increasingly flexible regulatory framework for the safe use of drones that encourages innovation, fosters informative journalism, and respects the First Amendment, and it should avoid unnecessarily increasing burdens or costs on journalists who rely on UAS to gather and report the news in the name of protecting the privacy of the public.

[2] *See* Dissent of the News Media Coalition to ARC Recommendations and Final Report to FAA Administrator Michael Huerta (Sept. 30, 2017).

The opportunities that drones afford are many. As predicted by both the government and the private sector, the FAA's Part 107 regulation has fostered rapid, significant innovation and growth in commercial and private unmanned aircraft systems. Drones today are powerful tools for safe and effective newsgathering, and they provide enormous public benefits. The Coalition appreciates the efforts of the FAA to create a regulatory framework that balances the First Amendment rights of journalists and the public with the need for safety and security.

Whether UAS are performing search and rescue missions, gathering news and enhancing the public's access to information, allowing farmers to be more efficient and environmentally friendly, inspecting power lines and cell towers, performing aerial photography to real estate and insurance service providers, 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.

The Coalition, however, is concerned that any attempt to create a federal statutory privacy framework for the operation of UAS would unavoidably, and impermissibly, constitute government surveillance of a journalist's drone operations in violation of the First Amendment. Allowing any more robust tracking of drones by law enforcement or the public than that currently contemplated by the FAA's Remote Identification rules could compromise journalistic independence and access, and increase the risk of harassment of news outlets and journalists on the ground.

Society is only just beginning to realize the full potential of UAS, and the use of drones for newsgathering is no different. We are seeing, time and again, how drones can be utilized to shed light on newsworthy events in a way, and on a scale, not previously thought possible. News organizations and individual journalists now use drones to cover natural disasters – from hurricanes, to volcanic eruptions, to wildfires – providing the world with access and perspectives that previously seemed prohibitively expensive or simply unavailable. These news stories not only serve journalists' audiences, but also fill a critical role in the emergency response system, allowing local law enforcement entities to enlist the help of journalists to provide vital, timely information to ensure public safety during crises.[3]

[3] In fact, in 2018, President Trump signed an omnibus spending bill that expanded the definition of "essential service providers" to include radio and television broadcasters in recognition of the critical role that journalists provide to the public during crises. As a result, broadcasters, cable and satellite providers are among those entities that have priority access to funding and resources through the Federal Emergency Management Agency during natural disasters in order to restore their services. *See* 42 U.S.C. § 5189e(a)(1)(A)(i); Davina

News organizations and journalists are dedicated to the safe and secure operation of drones, and they are demonstrating the many ways that drones can serve the public interest. In the years to come, they will no doubt devise innovative uses for drones that will result in even more impactful news reporting by informing the public, saving lives, and sharing important news. An increasingly flexible regulatory framework can both enhance the safety and security of drones while encouraging innovative and important journalism. The FAA must ensure that its rules do not impede innovation and that its rules continue to respect the protections of the First Amendment.

Privacy Concerns of Individuals and Communities are Already Protected by the Current Framework of State and Federal Regulations and Tort Law

This ARC has given significant consideration to privacy interests throughout the last many months, including convening a privacy task force during Phase 1 and returning to the question of privacy after three ARC members[4] raised additional concerns during Phase 2 of the ARC. At no time during the ARC, however, was "general consensus" reached regarding the recommendation that the FAA consider development of a privacy statute.

Rather, the Phase 1 Task Force recognized that although the privacy interests of individuals may be implicated by BVLOS operations, the FAA has historically concluded that the privacy interests of the general public are out of the scope of the FAA's directive. In addition, the Phase 1 Task Force agreed that the public should not have access to specific, identifying information about BVLOS operations, whether in real-time or more generally.

What appears to be motivating the few organizations who have expressed support for a new privacy statute seems to be concern that the public will not accept the presence of drones in their communities. In some respects, this is similar to the concern raised in 1888 regarding the introduction of the Kodak Brownie camera. The Kodak camera allowed, for the first time, anyone to take photographs in public places, as opposed to the controlled seclusion of photography studio. This sudden appearance and widespread use of the camera

---

Sashkin, *Repack Funds and First Responders – What Broadcasters Need to Know about the 'Omnibus' Spending Bill of 2018*, CommLawBlog, Mar. 23, 2018 (available at https://www.commlawblog.com/2018/03/articles/fcc/repack-funds-and-first-responders-what-broadcasters-need-to-know-about-the-omnibus-spending-bill-of-2018/).

[4] The ARC participants who raised privacy interests in the discussions were the American Civil Liberties Union, Electronic Frontier Foundation and Electronic Privacy Information Center.

caused the public to react with fear – many places posted signs banning the use of cameras, and newspapers ran stories about the dangers of public photography.[5]

Despite the concern surrounding this technological innovation, and rather than prohibit the use of cameras in public outright, over the past century and a half tort law developed to accommodate the legitimate interests in privacy and the public interest in a free and open society.[6] Additionally, states have developed codes to specifically proscribe unlawful surveillance through use camera technologies in private spaces.[7] Courts have had no trouble adapting both the common law and state codes to each wave of new technology.

Indeed, the FAA has, on several occasions, considered the issue of privacy in the context of UAS operations, and it has repeatedly concluded that the FAA is not authorized to

[5] "The Kodak Camera Starts a Craze," The Wizard of Photography, WNED http://www.pbs.org/wgbh/amex/eastman/peopleevents/pande13.html.

[6] *See, e.g.*, *Shulman v. Group W. Productions, Inc.*, 955 P.2d 469 (Cal. 1998) (filming accident victim at scene of accident was not intrusion of victim's seclusion, but victim would have reasonable expectation of privacy in rescue helicopter); *Eick v. Perk Dog Food Co*. 347 Ill. App. 293, 299 (Ill. App. 1952) (the right to privacy is a limited one in areas of legitimate public interest); *Tagouma v. Investigative Consultant Servs., Inc.*, 2010 PA Super 147, 4 A.3d 170, 174 (Pa. Super. 2010) ("there is no liability 'for observing [ ] or even taking [a] photograph while [a person] is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye."); *Martin v. Dorton*, 210 Miss. 668, 669, 50 So. 2d 391, 391 (Miss. 1951) (public officer cannot complain that his privacy has been invaded when his photograph is taken for publication in connection with a legitimate news story); *c.f. Souder v. Pendleton Detectives*, 88 So. 2d 716 (La. App. 1956) (using camera with telescopic lens to photograph bedroom from neighboring house).

[7] *See e.g.* Cal Pen Code § 647(i) ("Who, while loitering, prowling, or wandering upon the private property of another, at any time, peeks in the door or window of any inhabited building or structure, without visible or lawful business with the owner or occupant" is guilty of a misdemeanor); 11 De. Code Ann. § 1335 ("A person is guilty of violation of privacy when he (1) trespasses on private property intending to subject anyone to eavesdropping or other surveillance"); TCA § 39-13-605 ("It is illegal to knowingly and without consent photograph another person or cause him to be photographed in a place where there is a reasonable expectation of privacy if the photograph (1) would offend or embarrass an ordinary person if such person appeared in the photo and (2) was taken to sexually arouse or gratify another.")

craft privacy regulations.[8] Rather, the FAA has sensibly acted within its mandate to craft regulations that complement tort law and state regulations to ensure the safe and lawful operation of drones in our national airspace. It should continue to abstain from the development of regulation or statute in the name of privacy protection as it considers a rulemaking to authorize the operation of drones beyond visual line of sight.

As the Coalition has repeatedly stated, it does not object to the requirements contained in the FAA's Remote ID rules that each drone have a visible unique identifier, and that law enforcement and the public have a mechanism by which to verify that UAS operations occurring in their communities are lawful – but that is already contemplated by the current statutory framework. The rules enable the quick identification of drones that are behaving in suspicious, or illegal, ways, whether that be flying in a no-fly zone, near a restricted area, or behaving erratically. No additional federal statute is needed to properly protect the privacy interests of the public.[9]

Should the FAA Recommend Congress Adopt a Privacy Statute, it Must Contain Appropriate Safeguards to Preserve the First Amendment Interests in Newsgathering

The news media has a unique and nuanced relationship with law enforcement and the communities they serve. Journalists take seriously their role as the Fourth Estate watchdog on government, which requires that journalists at times investigate the conduct of government officials and law enforcement officers. In addition, journalists each day report on matters of concern in their communities. Any privacy statute that implicates the operations of newsgatherers has the very real potential to act as a de facto prior restraint on certain types of coverage and of increasing the risks to reporters doing their job, chilling the reporting of stories of great public importance.

---

[8] *See, e.g.*, Final Rule, *Operation of Small Unmanned Aircraft Systems Over People*, 86 Fed. Reg. 4314, 4365 (Jan. 15, 2021) ("Although the Agency is not authorized to impose regulations based on privacy concerns, the FAA has collaborated with the public, stakeholders, and other agencies with authority and subject matter expertise in privacy law and policy. As stated in the 2016 final rule, the FAA's mission is to provide the safest, most efficient aerospace system in the world, and does not include regulating privacy or free speech. Privacy issues are outside the focus and scope of the rule.").

[9] Indeed, the area where more transparency is needed, as the News Media Coalition has advocated in the context of other rulemakings, is for the FAA to require law enforcement to articulate grounds under a "probable cause" or "reasonable suspicion" to access personally identifiable information about drone operators. *See* Comments of the News Media Coalition, Docket No. FAA-2019-1100, Notice No. 20-01, Remote Identification of Unmanned Aircraft Systems (Mar. 2, 2020) at 8.

Under well-settled First Amendment law, the Government can impose reasonable time, place, and manner conditions on newsgathering, but only when those conditions are narrowly tailored to address a legitimate government interest.[10] Any statutory provision that governs privacy risks creating an unreasonable First Amendment limitation on the manner of operating a drone that is not narrowly tailored to a legitimate government interest.

Journalists' use of drones is in many ways unique when compared to the typical drone user. Whatever newsgathering tool they use, journalists have an utmost interest in conducting operations without surveillance by the government or by the subjects of their reporting. Across the Coalition, members have dedicated significant time, resources and training to ensure the safe and secure operation of drones in a manner consistent with the independence of the press guaranteed by the First Amendment.

Therefore, at a minimum, any new drone privacy regulation considered by the FAA must exempt news media operations. Indeed, the federal government included a similar carve-out for newsgatherers in the Voluntary Best Practices for UAS Privacy, Transparency, and Accountability, developed by the NTIA, a component of the U.S. Department of Commerce.[11] This carve-out states:

> **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

[10] *See McCullen v. Coakley*, 573 U.S. 464, 486 (2014) (content-neutral regulations "may not regulate expression in such a manner that a substantial portion of the burden on speech does not serve to advance its goals.") (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989)). For instance, effective January 1, 2020, a fixed wing or rotary wing aircraft operated by the news media must broadcast its location through Automatic Dependent Surveillance – Broadcast (ADS-B), if it intends to operate in certain restricted airspace, to maintain the safety of the NAS and the security of restricted airspace. 14 CFR § 91.225.

[11] *See* https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

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.

Indeed, current laws and regulations contain several similar examples that limit access to information about journalists' activities to instances where law enforcement is able to satisfy legal standards:

- The Privacy Protection Act, which governs the issuance of search warrants to journalists, provides that "it shall be unlawful for a government officer" to search or seize a journalist's work product unless "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate[.]"[12]

- Similarly, the United States Attorney General's policy regarding obtaining information from, or records of, journalists, applies in all instances except where the government has "reasonable grounds to believe that the individual or entity is", for example, "a member or affiliate of a terrorism organization."[13] Moreover, before authorizing a subpoena in a criminal matter, the Attorney General himself must articulate, among other requirements, "reasonable grounds to believe, based on public information, or information from non-media sources, that a crime has occurred[.]"[14] In fact, in July 2021, Attorney General Merrick Garland announced that the DOJ would end its use of "compulsory legal process for the purpose of obtaining information from or records of members of the news media acting within the scope of newsgathering activities," and he directed a comprehensive review of regulations to ensure that all regulations comport with the directive.[15]

Any statute that permits broader or unfettered real-time access to location and identifying information is unnecessary to protect the privacy interests of the public, and will impermissibly intrude on journalists' First Amendment rights to gather and report the news.

---

[12] 42 U.S.C. § 2000aa(b).

[13] 28 CFR § 50.10(b)(1)(ii)(B).

[14] *Id*. at (c)(4)(ii)(A).

[15] *Use of Compulsory Process to Obtain Information From, or Records of, Members of the News Media*, Office of the Attorney General (July 19, 2021), *available at* https://int.nyt.com/data/documenttools/attorney-general-memo-re-compulsory-process/862efd19514d7250/full.pdf.

Therefore, to the extent the FAA decides to consider a privacy statutory framework, it must carve out the activities of newsgatherers from that framework.

***

The Coalition appreciates the tireless efforts of the ARC leadership to consider and address the many important issues raised by the operation of drones beyond the visual line of sight. The Coalition is enthusiastic about the opportunities these types of operations will afford them to better tell the important stories of interest to their communities, and its members are committed to maintaining their reputation as respected and trusted operators of drones.

Sincerely,

Charles D. Tobin, Ballard Spahr LLP
Emmy Parsons, Ballard Spahr LLP
Joel Roberson, Holland & Knight LLP

On behalf of the News Media Coalition:

Advance/Newhouse Partnership
American Broadcasting Companies, Inc.
The Associated Press
Capitol Broadcasting Co.
Fusion Media Network
Gannett Co., Inc.
Getty Images (US), Inc.
National Press Photographers Association
NBCUniversal Media, LLC
News Media Alliance
The New York Times Company
The E.W. Scripps Company
Sinclair Broadcast Group, Inc.
TEGNA, Inc.
WP Company LLC

Exhibit B

Ballard Spahr LLP

EFF ELECTRONIC FRONTIER FOUNDATION

MEMORANDUM

TO ARC Security Subgroup

FROM Privacy and Data Sharing Task Group
Charles D. Tobin, on behalf of News Media Coalition
Andrés Arrieta, Electronic Frontier Foundation

DATE July 28, 2021

RE Privacy and Data Sharing – Recommendations for Phase 2

BACKGROUND

Framing the Scope of the Privacy Concerns

The Privacy and Data Sharing Task Force agreed that, as the FAA's Remote ID Final Rule acknowledged, there is an inherent tension between having the ability to identify UAS conducting BVLOS operations in order to engage in risk assessment and mitigation, versus the cost to privacy interests from increased transparency about UAS operations and operators.

As the ARC moves to Phase 2, the Privacy and Data Sharing Task Force urges the working group to keep at front of mind that new or enhanced security concerns from BVLOS should be addressed and mitigated through measured proposals that also protect privacy interests.

Categories of Privacy Concerns Relevant to BVLOS Operations

The Privacy and Data Sharing Task Force discussed three categories of individuals/entities whose privacy may be implicated by security concerns. These three categories include: (1) UAS operators, (2) UAS customers, and (3) the general public. As discussed below, however, the Task Force did not reach consensus on whether the privacy concerns of the general public are within the scope of this working group's directive.

1. *UAS Operators*

The Task Force agreed that privacy considerations of UAS operators fall within the scope of BVLOS security concerns. The Task Force also recognized, however, that there are several

layers to the privacy concerns of UAS operators based on (1) the type of operator and (2) the type of operation.

For example, "UAS Operators" can include both the pilot in control of the UAS while in flight, and, in many cases, the company behind the pilot. The Task Force agreed that in general, enhanced security risks from BVLOS operations may be mitigated by having greater transparency into the company that operates the drone without needing greater transparency into the identity of that company's specific UAS pilot.

In addition, the Task Force agreed that not all types of operations pose the same levels of security risks. For example, UAS operations to start controlled burns of forests are likely to raise greater security concerns than UAS operations to deliver grocery items or to conduct newsgathering operations. Any BVLOS regulations should ultimately account for these varying degrees of security and privacy concerns.

2. *UAS Customers*

The Task Force agreed that privacy considerations of UAS customers fall within the scope of BVLOS security concerns. Customers include those who receive a service via UAS operation, for example, an individual who receives a prescription via drone.

The Task Force agreed that a presumption of privacy should favor minimal data gathering and intrusion into customer privacy absent an actual, articulated security risk. For example, the frequency with which a household receives package deliveries is not generally relevant to mitigating a security concern.

The Task Group questioned, but did not come to a conclusion, regarding where the responsibility or burden should lie for gathering, and making transparent, any customer data. Possibilities include the FAA, the drone operator or the customer.

3. *General Public*

The Task Force considered whether the general public's privacy concerns are within the scope of BVLOS security considerations. For purposes of this discussion, the general public includes those individuals in areas with BVLOS operations who are not directly involved in such flights.

With respect to certain categories of BVLOS operations, including First Amendment and civil liberties use cases such as newsgathering operations and political activism, the Task Force agreed that the privacy considerations of the general public are not within the scope of BVLOS security concerns. That is, because of the constitutional implications of journalism and political activism, the privacy interests of the general public in the vicinity of these operations are out of scope, and to the extent general public privacy is brought within the scope of Phase 2 considerations, these activities should be carved out from that discussion.

The Task Force also discussed the history of the FAA's position regarding regulation of privacy in the rulemakings for Part 107, Remote ID and Surveillance, and Flight Operations

Over People. The Task Force acknowledged that in these prior rulemakings, the FAA determined that the privacy of the general public was out of scope. The Task Force did not, however, reach consensus as to whether BVLOS operations warrant the FAA's reconsideration of these past decisions, but agreed that given the time constraints of this ARC, this process is not suited for drafting comprehensive privacy laws.

A portion of the Task Force remains concerned about the privacy implications, which it views as an enhanced security risk from expanded BVLOS operations related to: (1) the activities of law enforcement, (2) the collection and storage of data (whether intentional or inadvertent) during delivery operations, and (3) any information-sharing agreement between law enforcement and commercial drone operators.

Information Sharing and Access

The Task Force addressed access to identifying information regarding UAS operations by (1) law enforcement, and (2) the general public. The Task Force also considered the different privacy considerations regarding access to that information in real time versus access to more static information, including the Part 48 (registration and marking requirements for sUAS) database that could allow law enforcement or the public to understand the operations that have been authorized in a particular community.

The Task Force agreed that the general framework established by the Remote ID final rule, session ID + Part 48 database, is generally reasonable. The Task Force considered that it is likely that the final BVLOS rule will require additional information of operators seeking to conduct BVLOS operations, and that it will likely be tempting to include that additional information in the Part 48 database. The Task Force considered that it may not be necessary to include all additional information in order to mitigate security concerns, and that limiting the scope of information in the Part 48 database is desirable to mitigate the privacy intrusion by the FAA and law enforcement to specific operations. For example, the Task Force agreed that being able to identify which UAS belongs to which operator, and which type of operation(s) that UAS has been cleared to conduct, is likely sufficient information to enable the FAA and law enforcement to identify security concerns.

The Task Force agreed that any Trusted Operator framework should include heightened requirements and consideration to ensure that such operations pose little security risk to communities. In exchange, UAS operations so certified should receive the benefit of heightened privacy and less intrusion by either law enforcement or the general public into their identifying information. The Task Force agreed that this possibility of greater privacy could incentivize more operators to obtain this certification, which would, in general, mitigate overall security concerns with expanded BVLOS operations.

The Task Force also agreed that, as with the Remote ID Final Rule, the public should not have access to specific, identifying information about BVLOS operations, whether in real-time or more generally.

PHASE 2 RECOMMENDATIONS

1. Acknowledge the inherent tension between transparency for the sake of security and the cost to privacy interests as a result of that transparency. Be mindful when developing specific policy recommendations and be willing to tolerate some level of risk in order to preserve some degree of privacy for the operator and the operation;

2. Develop a security framework that reflects different standards of transparency for different types of operators and different types of operations;

    a. Consider that the purpose of the operation should be accounted for in weighing transparency versus privacy concerns: the more benefit a specific BVLOS operation, or category of BVLOS operation, affords to society, the more "risk" the public should be willing to assume as it relates to preserving privacy, unless that benefit includes obvious risk (i.e., controlled forest burns).

3. Consider whether hobbyist BVLOS operations warrant any different, or additional, security-mitigation measures. Whereas commercial UAS operators have an incentive to be "good actors" in order to maintain their certification, hobbyists may be more likely to pose security risks, whether inadvertently or deliberately, and as such, may warrant more transparency regarding their BVLOS operations.

4. Support a presumption of privacy for UAS customers, but identify those types of UAS customers who pose a greater security concern and warrant heightened transparency. Phase 2 should consider:

    a. The type of activity being conducted on behalf of the customer;

    b. The extent to which even seemingly innocuous information, like flight paths, could be triangulated and correlated in a way that intrudes on customers' privacy for low-risk BVLOS operations; and

    c. Who should bear the responsibility and burden for gathering, and making public, any customer data that must be made public. The FAA? The drone operator? The customer?

5. Refrain from writing privacy laws, but consider the following:

    a. Carving out newsgathering operations and political activism activities from any new consideration of general public privacy, in light of the First Amendment interests;

    b. Consider adding certain requirements, such as proportionality, data minimization, privacy impact reports, and guidance regarding which privacy issues should fall within the FAA's purview to regulate and which should be deferred to other agencies and communities; and

c. Direct the FAA to require operators to stay within the parameters of operations outlined in their authorization (i.e., no inclusion of sensors that could be used for surveillance but have nothing to do with the intended operation).

6. Support development of a Trusted Operator Framework:

    a. Such a framework should include heightened requirements and approvals that are a "meaningful bar" so that communities have confidence that such operations pose a low security risk;

    b. In exchange for obtaining the Trusted Operator certification, such operations should be protected by a higher threshold before law enforcement can access identifying information, such as "probable cause" or "reasonable suspicion"; and

    c. The framework should include parameters for when and how a Trusted Operator would lose its status.

7. Consider the privacy interests in UAS operators' personally identifiable information (PII), and create a framework that restricts access to PII by law enforcement and the general public:

    a. Law enforcement may need access to identifying information, but Phase 2 should support tighter restrictions on this access, for UAS operators who complete the Trusted Operator process, beyond the provisions in the Remote ID final rule

        i. Trusted Operator operations should be subject to a heightened "probable cause" or "reasonable suspicion" standard before law enforcement may access PII; and

        ii. Not all additional information gathered for BVLOS certifications or Trusted Operator applications should be included in the Part 48 database; being able to identify which UAS belongs to which operator, and what type of operation(s) that UAS has been cleared to conduct is likely sufficient for identifying security threats;

    b. As with Remote ID, the public should not have access to PII regarding UAS operations, and there should remain barriers to accessing PII by the public;

        i. But the general public should have available a process to report an actual, articulable security concern related to a specific BVLOS operation and receive reassurance in real-time or near-real time, that the operation is lawful.

8. Support inclusion of a provision in the final rule that any law enforcement inquiries into PII of UAS operators are subject to FOIA:

    a. The public should be provided with insight into whether law enforcement is abusing its ability to gather information about UAS operations under the guise of new or enhanced security/law enforcement concerns from BVLOS.

Exhibit C

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**