Privacy Considerations for BVLOS Drones:

Privacy Considerations for FAA Aviation Rulemaking Committee on Beyond Visual Line of Sight Drone Flights

Arrieta Andrés, Scott Jeramie, Stanley Jay

Authors: Arrieta Andrés, Scott Jeramie, Stanley Jay

A publication of the American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center, 2021.

December 2021

Introduction

Our organizations recognize the many potential positive uses to which Beyond Visual Line Of Sight ("BVLOS") drone flights could be put. But it is also our job to consider some of the implications that a regime of routine and scaled BVLOS flights could have for privacy and surveillance, how such a regime could harm Americans' privacy, and what the pathway is for ensuring that we can maximize the benefits of this technology while minimizing the harms.

Why addressing privacy is important

Drones are very powerful surveillance platforms that greatly increase the ease and possibility of aerial surveillance. As drone technologies advance, drones will be able to fly longer and farther, carry heavier and more diverse payloads of surveillance equipment, and become even more capable of autonomous operation—all at an increasingly cheaper price point. The operational flexibility of duration, distance, and altitude makes it harder for people on the ground to detect and understand what is happening with a particular surveillance drone.

Drones can carry numerous surveillance technologies

Most drones by default are equipped with cameras that can record images or take pictures. These cameras can be quite powerful. Even consumer drones can come equipped with cameras with the ability to shoot in 4K, and military drones carry gigapixel cameras that can photograph city-sized areas.

Cameras are not the only technology that can be added to drones, of course. Drones are a platform, and the only limits on what they can carry are size and weight. Among the sensors that can be attached to drones are microphones, heat and movement sensors, mobile phone interception devices (aka IMSI catchers), GPS, radar, Lidar, sonar, range-finders, magnetic-field change sensing, radio frequency sensors, and chemical and biochemical sensors. Data from drone surveillance can be combined with other surveillance technologies such as facial recognition and license plate readers or correlated with data from surveillance technology on the ground or online to identify people and vehicles, track their movements across time and space, or analyze their associations or habits. The lack of rules concerning drones and the technology they can carry means there will be vast opportunities for surreptitious data collection from the public.

Drones increase the risk of aerial surveillance

The lack of legal protections against aerial surveillance combined with the lowered bar for entry that drones create for aerial surveillance, raises the risk of privacy invasions. The law of aerial surveillance of public spaces is murky at best and is not well enough developed to protect the public in the face of the broad availability of drones.

Drones make it cheaper and easier to conduct aerial surveillance. Drones are generally orders of magnitude cheaper than other aircraft capable of conducting aerial surveillance (i.e. airplanes and helicopters). Drones are much cheaper to maintain and don't require the same level of training to operate as do crewed aircraft making the cost of the "pilot" much cheaper. Drones are increasingly equipped with technology to steady their flight, hover in one place, and avoid crashing into objects. Many consumer drones can track specific objects on the ground or can be programmed to fly a specific flight path.

Additionally, advancing drone technology will allow for semi-autonomous or even completely autonomous drone operations, removing the need for a pilot at all. This allows a single person to oversee multiple drone flights at once—making it even easier and cheaper to operate a drone. Autonomous BVLOS drone operations, in particular, will enable widespread drone surveillance in ways that manual line of sight drone operations could not.

Protecting the public's expectation of privacy

Members of the public are not in a position to know if their privacy is being compromised by drone surveillance, and even if they were they would have no recourse. How is someone currently supposed to know if they or their community is subject to drone surveillance? Drones can be hard to detect, flying high enough to make spotting them visually or hearing them above ground noise next to impossible.

Even if someone does become aware that a drone is nearby, there is currently no practical way to know what surveillance capabilities it possesses or if it is actively collecting information. There is no consistent and clear way to know if the drone is a government, commercial, or private drone or what its purpose is. When it comes to protecting privacy from drone surveillance, the public is largely at the mercy of drone operators.

Protecting the public's expectation of privacy from drone surveillance and preventing privacy violations will facilitate acceptance of drones in the National Airspace. The public is wary of drones[1] and will only become more so when BVLOS drone operations

1 DACUS, Drones and Drone Operations – Citizen's Perspective: Representative population survey on the acceptance of drones and the social impact of drone operations in urban areas (2021), https://dacus-research.eu/wp-content/uploads/2021/08/D5.1-Social-Acceptance-Survey-Results.pdf; Terance D. Miethe, Ph.D. et al., UNLV Center for Crime and Justice Policy, Public Attitudes about Aerial Drone Activities: Results of a National

start occurring in populated areas. And too often, a disproportionate amount of the negative impact of new technologies falls on the most vulnerable and marginalized communities[2]. Without privacy protections in place, drone incidents violating people's privacy will taint the whole industry. A few bad actors could seriously hamper integration of drones into the airspace, especially for BVLOS flights. Protecting everyone's privacy, but particularly that of vulnerable and marginalized communities, will speed up acceptance and integration of drones.

Categories of privacy invasion

Given the vast range of creative uses to which a generative technology such as BVLOS drones could be put, it is impossible to anticipate all the ways that the technology might be used to violate privacy. Some potential concerns, however, fit into the following categories:

Individual privacy-invading operators

BVLOS operations may eventually become relatively common, widespread, and democratized, as the barriers to entry continue to fall. If the FAA achieves its goal of allowing by-rule BVLOS flights[3], and such a general rule doesn't include privacy protections, we are likely to see BVLOS drones used for aerial reconnaissance in privacy-offensive ways. For example, drones might be used to follow other people for extended periods of time and/or across extended distances. People might follow the car of a celebrity, their ex-wife's new boyfriend, a driver that one is angry at, or an attractive person as they complete their jog.

Corporate privacy invasions

If BVLOS flights are permitted by any operator complying with a rule, numerous uses of such flights will emerge that have significant privacy implications. In today's world, data is worth money, so there will be constant market incentives to maximize privacy-invasive aerial data collection practices.

Possible privacy-invasive uses of BVLOS drones include:

- Collecting data on traffic or pedestrian patterns across a town or city, both aggregated and individually targeted.
- Measuring home occupancy rates by surveying which houses are lit up or heated in the visual or infrared spectrum, and when and to what degree, or by

Survey (July 2014), https://www.unlv.edu/sites/default/files/page_files/27/PublicAttitudesAboutAerialDroneActivities.pdf;Paul Hitlin, 8% of Americans Say They Own a Drone, While More Than Half Have Seen One in Operation, Pew Research Center (December 19, 2017), https://www.pewresearch.org/fact-tank/2017/12/19/8-of-americans-say-they-own-a-drone-while-more-than-half-have-seen-one-in-operation/.

2 Nathan Sheard & Adam Schwartz, Community Control of Police Spy Tech, Electronic Frontier Foundation (May 19, 2021), https://www.eff.org/deeplinks/2021/05/community-control-police-spy-tech.

3 Currently, anyone wanting to fly BVLOS has to apply for special, individualized FAA permission. By-rule flights would allow any party to carry out a BVLOS flight as long as they comply with the rules.

measuring the amount and type of vehicles parked outside at different times and days.
- Following randomly selected customers home from a store or restaurant to get a sense of where their customer base is coming from.
- Collecting information about homes and their owners for marketing purposes, such as who owns a backyard grill, who has a neat garden and who doesn't, or who could use some roof repairs.
- Intercepting cell phone signals using IMSI catchers (aka "Stingrays") to collect location data or other information that can be associated with specific people through the unique identifiers of cellphones.
- Collecting WiFi identifiers to correlate online profiles to individuals' physical locations.

There could also emerge many other privacy-invasive uses yet to be conceived of. The companies that are operating the most flights with the most time in the air might be in an especially good position to collect data that, because of its greater comprehensiveness, would be all the more valuable.

While effective transparency measures could create reputational and market pressures against such data collection, much surveillance is silent and invisible. If a company engaged in delivery operations, for example, decided to use those delivery flights to collect information on people along flight paths, those people might never know.

Mass surveillance

These kinds of privacy-sensitive commercial uses could be pushed to extremes if companies or services emerge that use rotating parallel flights to create 24/7 wide-area surveillance of cities and towns. Such a wide-area surveillance service is already being pitched to police departments (none of which have adopted it, partially due to community opposition as well as a successful ACLU constitutional challenge[4]). But similar services could establish private markets for such surveillance, for example by selling to insurance companies, real estate firms, and others.

Law enforcement

Law enforcement uses of drones raise many issues, including routine surveillance and tracking; the retention and sharing of imagery, including incidentally collected imagery; discriminatory deployments; the potential for abuse; and use in automated

4 Saira Hussain & Hannah Zhao, Victory! Fourth Circuit Rules Baltimore's Warrantless Aerial Surveillance Program Unconstitutional, EFF (July 2, 2021), https://www.eff.org/deeplinks/2021/07/victory-fourth-circuit-rules-baltimores-warrantless-aerial-surveillance-program.

enforcement. The ACLU[5], EFF[6], and EPIC[7] have all made recommendations for checks and balances on law enforcement's use of drones.

Unwanted intrusions

Even in the absence of unwanted collection of personal information or the like, many people will resent the presence of video cameras hovering in the air over their heads, especially around their homes. Whether a drone has a camera or other potentially intrusive sensors on board may not matter; it is a well-established principle of privacy that people are just as affected by the possibility[8] that they are being watched as they are by actually being watched. This kind of privacy invasion involves a diffuse set of feelings that combines the dislike of being watched, intrusion upon seclusion, spoliation of environment, intimidation, nuisance, and noise. We strongly suspect that the frequent incidences of "drone rage" that have been experienced in the drone community reflect this cluster of feelings.

To the extent the kinds of invasions take place, that will only intensify this set of negative feelings towards drones.

There is a strong possibility that routine and scaled BVLOS operations, especially package delivery, will increase the public's exposure to drone operations over time. Today's relatively rare line-of-sight operations will become tomorrow's daily or even hourly BVLOS operations over or near people's homes, especially if they find themselves situated in a flight pattern or chokepoint. It's possible that drones will initially be welcomed as a novelty but will quickly wear out their welcome.

The FAA's role in addressing privacy risks

From the beginning, FAA recognized the importance of addressing privacy to facilitate the integration of drones into the National Airspace. Soon after the FAA Modernization Act of 2012 was passed, then Representatives Ed Markey and Joe Barton, the Co-Chairmen of the Bi-Partisan Privacy Caucus, sent a letter to the Acting FAA Administrator, Michael Huerta, to "express our concerns about the [FAA Modernization Act's] potential privacy implications and to request information about how the FAA is addressing these important matters."[9] Markey and Barton stated:

5 Jay Stanley & Catherine Crump, Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft, ACLU (Dec. 2011), https://www.aclu.org/sites/default/files/field_document/protectingprivacyfromaerialsurveillance.pdf.

6 Letter from Jennifer Lynch, EFF Staff Attorney, to Lieutenant Governor Mead Treadwell & Mr. Robert Davis (May 31, 2013), https://www.eff.org/files/eff_asa_model_drone_legislation_letter.pdf.

7 Use of Unmanned Aerial Vehicles (Drones): Hearing Before the Majority Policy Comm. of the Penn. State Senate (Mar. 15, 2016), (statement of Jeramie D. Scott, EPIC Director of Domestic Surveillance Project), https://epic.org/privacy/drones/EPIC-Drone-Testimony-20160315.pdf.

8 Karen Gullo, Surveillance Chills Speech—As New Studies Show—And Free Association Suffers (May 19, 2016), https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association.

9 Letter from S. Markey & Rep. Barton, to Michael P. Huerta, Fed. Aviation Acting Admin. (Apr. 19, 2012), https://irp.fas.org/congress/2012_cr/drones041912.pdf.

> "Now that the FAA has initiated the rulemaking process for implementing the FAA Modernization and Reform Act, the agency has the opportunity and responsibility to ensure that the privacy of individuals is protected and that the public is fully informed about who is using drones in public airspace and why.[10]"

The FAA responded by stating that "[t]he FAA recognizes that there are privacy concerns related to UAS operations, and the agency will review these concerns in the context of the ongoing UAS rulemaking activities and integration plans."[11]

The FAA's Comprehensive Plan and Roadmaps for drone integration have repeatedly recognized privacy as a key issue. In the Comprehensive Plan to guide the integration of drones required by the 2012 act, the FAA stated that "[m]embers of the NextGen SPC [Senior Policy Committee] agree on the need to address privacy concerns of the public at large while safely integrating UAS in the NAS."[12] All subsequent versions of the Roadmap also speak to the importance of addressing privacy with the most recent one stating:

> "The public has real concerns regarding UAS operations with respect to safety and privacy. If people don't feel safe when drones are operating around them, or they have persistent fears of drones intruding in their private lives, then UAS commercial opportunities will be very limited."[13]

As the FAA has made clear, the public acceptance of drones is required for the integration of drones into the national airspace, and the public will not accept drones if privacy is not addressed. As the agency overseeing the integration of drones, the FAA must make sure that there is a pathway for addressing ongoing privacy risks and new ones as they emerge.

Considerations in addressing privacy risks

Community response to drones

One of our biggest concerns is that an FAA BVLOS regulation will leave no room for addressing privacy problems that emerge with the technology. The FAA must not preempt localities from restricting BVLOS flights to address privacy invasions, whether or not the FAA decides to protect privacy in a rulemaking opening the skies to by-rule operations.

The truth is that we don't know to what extent communities will want or accept regular or frequent drone flights, or where, or under what conditions. That will depend on a

10 *Id.*

11 Letter from Fed. Aviation Acting Admin., Michael P. Huerta, to S. Markey (Sept. 21, 2012).

12 JOINT PLAN. & DEV. OFF., UNMANNED AIRCRAFT SYSTEMS (UAS) COMPREHENSIVE PLAN (Sept. 2013), 7, https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.

13 Fed. Aviation Admin., Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap (3rd ed. 2020) at 21, https://www.faa.gov/uas/resources/policy_library/media/2019_UAS_Civil_Integration_Roadmap_third_edition.pdf

complex and unpredictable set of often contradictory factors, ranging from whether the technology's benefits are broad and substantial or narrow and overblown, to people's feelings about the technology's safety, to their feelings about the full range of possible privacy invasions discussed above.

From its perch in Washington DC, the FAA should not try to anticipate what all of those privacy problems will be in the coming years and decades, and how all communities will feel about them, and what kinds of restrictions or regulations are needed to solve the conflicts to the satisfaction of all kinds of American communities. It should not treat drones like crewed aviation, and impose a uniform set of drone rules across the entire country that preempts all state and local rules and thereby grant anyone a by-rule right to fly over communities.

With drones flying under 400 feet, a single nationwide rule is not likely to work in the way it does for crewed aviation. Crewed flights are generally too high to trouble most people. Noisy and camera-carrying robots flying in and through Americans' communities will be a whole new ballgame. The issues and controversies that have surrounded aircraft noise around some airports may emerge in every small neighborhood, albeit driven by more than noise. When residents feel there is too much wheeled vehicle traffic or traffic noise at their home, they can call up members of their city council and push to lower the speed limit, or install speed bumps, or make the street one-way. When the equivalent neighborhood complaints arise over drone flights, people should not have to call up the federal government. That is a recipe for political disaster, both for the FAA and for those who wish to see drones succeed at the things they may be well-suited to do.

Most Americans don't give much thought to drones. Most of those who are thinking about the technology today are excited about and invested in them, either emotionally or financially. But we don't want to see drones imposed on unwilling communities in disruptive and inequitable ways as Robert Moses[14] did with highways, acting out of a misguided modernist vision of what "the future" looks like, or on behalf of companies that stand to profit despite community desires and the public interest.

A better path is to allow communities to restrict drone flights in their jurisdictions (subject to limitations imposed by the First Amendment, as discussed below). This will allow accommodations between the various competing equities in drone deployment (privacy, noise, commerce, convenience, environment, etc.) to emerge organically as diverse communities react in different ways to the technology. If the technology proves practical, useful, and popular, then communities that are overly restrictive will quickly come to feel that they're missing out. If, as a practical matter, drones just don't work out for many of the uses now envisioned, or their downsides are starker than boosters hope, then they will recede into the niches where their advantages are greatest and downsides the smallest without degrading the quality of life of American communities.

The privacy problems and conflicts drones are likely to spark are diverse and unpredictable. While nationwide rules make sense in many areas such as safety and

14 Wikipedia, Robert Moses (Last modified Nov. 14, 2021), https://en.wikipedia.org/wiki/Robert_Moses.

transparency, reasonable community control is not only the best way to honor the concept of democratic control over our quality of life, but also the best way to address privacy and other problems that emerge, while avoiding over-regulating to protect against privacy harms that never materialize.

First Amendment considerations

The potential for drone photography as a tool for art, journalism, and activism is significant. The First Amendment generally protects the gathering of news and other information of importance to the public, and specifically protects photography as a means of expression and as a way of gathering information. In general, a person in a public place where they have a right to be may make photographs of anything that is in plain sight. But the First Amendment does not necessarily create a right to operate a BVLOS drone, or to operate one wherever one wants, just because BVLOS drones can be used to make photos.

One thing the First Amendment generally does not permit is for the government to restrict drone flights according to the identity of the photographer or the subject of their photography. It also bars government actors from blocking drone photography of their activities just because it is politically inconvenient or embarrassing. Nor does it allow wide-ranging bans on photography of "critical infrastructure."[15] It may allow bans on drone flights near certain critical infrastructure for safety purposes (though there will be a constant temptation, which some will inevitably give in to, to use safety as a pretext for enacting such bans).

Remote ID

The remote ID requirement is one of the best opportunities for the FAA to implement privacy-related rules that will facilitate the public's acceptance of drones. A key aspect of addressing privacy concerns is to make sure people have the means to know when drones are flying in their proximity and who is flying them. Identification is important because accountability is very hard without it.

Remote ID can also facilitate much-needed transparency. Remote ID is the avenue by which the public can learn about not only what drones are flying near them, but additional information including the surveillance capabilities of the drone, the purpose of the drone, and the information the drone might be collecting.[16]

For the Remote ID requirement to mitigate the privacy risks of drones, the requirement must be usable and useful to the public. It should not be complicated for members of the

15 Ari Rosmarin, Drone Rules Are Already Colliding With The First Amendment, ACLU (July 16, 2015), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/drone-rules-are-already-colliding-first-amendment

16 EPIC et al., Comments on the Noticed of Proposed Rulemaking: Remote Identification of Unmanned Aircraft Systems, Federal Aviation Admin. Docket No. FAA-2019-1100 (Mar. 2, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-et-al-Comments-FAA-Remote-Drone-ID-March2020.pdf.

public to identify nearby drones — it should be as simple as downloading a free app to one's phone and opening it up. And the Remote ID's range should be robust enough to give meaningful information about the number of drones in the area at a given time. Generally speaking, if the average drone is within range to collect information about a person or their immediate surroundings, then the Remote ID should have an equivalent range.

The Remote ID should directly or through an easily accessible database provide information about the drone's capabilities, purpose, and operation. This should include the type of surveillance technology on the drones and the purpose of the flight (e.g. package delivery). Drones should be identified as government, commercial, or non-commercial private. For government and commercial drones, the agency or company operating the drone should be made available. Additionally, Remote ID should allow easy access to details about the drone's operation, including what data the drone is collecting, what the data will be used for, and how long the data will be retained.

Network Remote ID, however, which would require every drone to have cellular capability and connect to the Internet to report its location in real time, does not strike the right balance between security, the privacy of those on the ground, and the privacy of drone operators. It would create a nationwide "bird's eye view" of every drone that flies, and under some proposals would give not only law enforcement exclusive access to that data, but also certain private-sector service providers. That would give those companies access to vast amounts of drone-flight data that they could use in unfair ways. For example, it might allow them to secretly gather data about consumer or commercial use of drones that would not be available to others, or to monitor drones that are being flown by a union with which the company is currently battling.

Recommendations

Requirements the FAA should implement

Transparency requirements

Transparency is a fundamental element of acceptance of drone BVLOS operations by the public. It allows the public and agencies to hold operators accountable and is a crucial means by which the public can exercise its rights.

When operating an aircraft, the operator should understand the risks that such operation imposes to the National Airspace System as well as to those on the ground—whether safety impact, noise, or environmental. By the same token, operators should also assess the impact of their operations on the public's privacy. Privacy impact assessments are a routine requirement for many government information collection processes, and increasingly for some companies as well. We would like to see a similar requirement imposed on government and commercial BVLOS operations in the national

air space. These reports should be easily and freely available to the public, and should include details such as:

- Type and Purpose of the drone operation. The operator should detail the purpose of its operation, so the public can understand its nature and also hold them accountable for mission creep, or covert-deceitful uses.
- Technical Capabilities. This should include not only the operational capabilities of the aircraft (distance, time, altitude, payload weight, etc.) but also the sensors on board, their capabilities, and the data collection they will be engaging in. For example, if the drone carries cameras, this data would include the power of any zoom lens and how that zoom is controlled (automated processes or remote operator), the camera's resolution, the camera's spectral range, and any live AI or analytics capabilities that it uses.
- Data collected. Detail of data collection that will occur during the operation. For example, if video will be collected, this would include information on when that video will be collected.
- How that data is used. The intended use of the data, for example, for navigational purposes, detection and avoidance of obstacles, infrastructure inspection, etc.
- Data disclosure. Who, other than the operator, can access the data, or with whom will it be proactively shared, and for what purpose.
- A privacy impact assessment. An assessment of how the operation, with the sensors, data collection, and sharing that it involves, will affect the communities over which this operation will take place, and what mitigations are in place to address these issues.

Community involvement requirements

- The FAA should allow localities to set their own rules in order to protect privacy or other values and to encourage local innovation.
- The FAA should ensure that there is enough transparency regarding drone flights that communities can make informed decisions about what kinds of operations they want to permit.
- The FAA should create ongoing mechanisms for individuals to raise concerns with the FAA, submit complaints, or report privacy invasions that they have experienced from drone operations (as well as noise and safety problems).

Remote ID requirements

The FAA must implement a program of Remote ID that empowers people on the ground to obtain key information about BVLOS drones in their vicinity. It should not implement a system for centrally tracking all drone flights across the nation.

Additional requests

- Minimization requirements. Congress must require government and commercial BVLOS operators to minimize the data collected, used, and shared to what's relevant and necessary to the operation described in their public statements. For

example, if a BVLOS drone is doing delivery, no data can be collected that is not strictly necessary to achieve that purpose, and video and image data collected for that purpose cannot be retained or used for other purposes like mapping services. Where appropriate this mandate should also include use of technical means of minimizing data collection. For example, a drone conducting a safety assessment of a railroad could electronically block out the portion of the video that includes the backyards of neighboring homes

- Additional stakeholder processes. We applaud the FAA for recognizing the need to expand the scope of the stakeholders participating in the Advisory Rulemaking Committee process, and for inviting privacy advocates to contribute their views in this Aviation Rulemaking Committee. It was often difficult for non-aviation stakeholders to participate in the process however, and we recommend that the agency consider convening a separate ARC or other proceeding through which to gather community, privacy, and other non-industry, non-aviation stakeholder input and perspectives. Future ARCs on the ongoing integration of drones into the national air space might also be structured to allow such perspectives to have separate conversations on questions that they themselves define.