COMMENTS OF THE AMERCIAN CIVIL LIBERTIES UNION

AND

ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL AVIATION ADMINISTRATION

Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations

[Docket No. FAA-2025-1908; Notice No. 25-07]

October 6, 2025

INTRODUCTION

By notice published August 7, 2025, the Federal Aviation Administration ("FAA") issued a notice of proposed rulemaking regarding the normalization of Beyond Visual Line of Sight ("BVLOS") drone operations.[1] The FAA's proposed rule would allow drone operations to expand and for drone operators to better take advantage of the potential of drones. But drone operations are not carried out in a vacuum, they take place in the real world where people and communities will be affected by the increased number of drones flying over their heads. If BVLOS drone operations are to thrive, the FAA must consider the surveillance implications of routine and scaled BVLOS flights, how such flights could harm Americans' privacy (real or perceived), and what is required to maximize the benefit of drones while minimizing the privacy harms. The agency must also consider the free expression implications of the technology.

BVLOS operations increase the potential for aerial surveillance and thus increase the risk to Americans' privacy

Drones are essentially aerial surveillance platforms capable of carrying a variety of different surveillance equipment. This makes their surveillance potential vast, with that potential growing sharply as the technology continues to advance. Under these proposed rules, drones will be able to fly longer and farther, carry heavier and more diverse payloads of surveillance technologies, and become increasingly more capable of autonomous operations. The increasing capabilities and likely lower costs of BVLOS operations will lead to more drones in the air. That will mean greater opportunities for operators to collect data on the public — and regardless of how much people are being watched, without proper privacy assurances the public perception will likely be that they are.

---

[1] *Notice of Proposed Rulemaking: Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight*, 90 Fed. Reg. 38212 (Aug. 7, 2025) [hereinafter *BVLOS NPRM*].

Drones are aerial surveillance platforms

One of the defining traits of most drones is the camera. It is why, when someone references "eyes in the sky," a drone is what often comes to mind. And the cameras on drones, even consumer drones, are quite powerful, often possessing the ability to shoot in high resolution and with powerful zoom lenses. But cameras are not the only technology that drones can be equipped with. Drones can carry microphones, heat and movement sensors, mobile phone interception devices (cell-site simulators aka "Stingrays"), GPS, radar, Lidar, sonar, range-finders, and radio frequency sensors, among many other technologies. Facial recognition technology and license plate reader technology can be used in conjunction with aerial cameras. And the data collected by drones can be combined with data from other sources to identify people, track their movements, and analyze their habits and associations. Given the lack of protections in place, the risks that some or all these technologies will be deployed on drones is real.

The U.S. lacks regulations to protect people's privacy from drone 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 case law on aerial surveillance of public spaces is murky at best and will not meaningfully protect the public from drone privacy invasions. Congress and the FAA have so far failed to implement adequate privacy protections against aerial surveillance. Moreover, neither states nor the federal government have established privacy laws that could serve as a backstop against drone surveillance. While around 20 states have passed consumer privacy laws, they are premised on ineffective "notice and consent" regimes with no meaningful limitation on the data that drone operators collect.

BVLOS operations will be resisted if people's expectation of privacy is not protected

Given the surveillance capabilities of drones combined with the lack of privacy protections and the lack of transparency, people are rightfully skeptical of drones. This was no better demonstrated than by the mass hysteria over a rash of purported drone sightings in New Jersey.[2] The lack of protections and transparency led to wild speculation about who was operating the drones and what they were doing — with some attributing the drones to foreign agents or secret U.S. government operations.

There have been incidents of homeowners, firefighters, and sports crowds illegally shooting drones out of the sky.[3] The FAA itself has reported that many concerned drone operators have

[2] Dave Collins, Mystery drone sightings continue in New Jersey and across the US. Here's what we know, AP (Dec. 20, 2024), https://apnews.com/article/drones-new-jersey-what-to-know-e6f565f5d51d9d47ad140e7e7d131842.
[3]Andrew Wolfson, 'Drone Slayer' suit could set US law, Courier Journal (Jan. 18, 20216), https://www.courier-journal.com/story/news/local/2016/01/14/suit-over-shot-down-drone-could-set-us-law/78651710/; Michael Zhang, Firefighters Try To Shoot Down Camera Drone with Their Hoses, PetaPixel (June 5, 2015), https://petapixel.com/2015/06/05/firefighters-try-to-shoot-down-camera-drone-with-their-hoses/; Joseph Serna and Brian Bennett, Mystery surrounds drone that flew above L.A. Kings victory party, L.A. Times (June 16, 2014), https://www.latimes.com/local/lanow/la-me-ln-kings-game-drone-no-owner-20140616-story.html.

"provided examples of confrontations, threats (including threats with firearms), and assaults that they or others have received during operations."[4]

The public is currently not in a position to know if their privacy is being compromised when a drone flies overhead —no meaningful way to know what surveillance capabilities the drone above them has, what information the drone is collecting, or how that information is going to be used. There is no way to know if the drone is a government, commercial, or private drone, or to know its purpose.

Given the real and perceived privacy risks that drones pose, it should come as no surprise that multiple studies of the public perception of drones have cited privacy as one of the main public concerns when it comes to integrating drones into the airspace. These studies have looked at issues like the general public's acceptance of drones,[5] the perception of delivery drones,[6] and the use of drones in urban areas.[7] An academic article reviewing the literature on the factors for the acceptance of drones by the public found privacy to be one of the main perceived risks of drones in the airspace.[8]

The FAA is well aware of the public's privacy concerns. In the agency's Roadmap regarding integrating drones into the National Airspace, the FAA concedes:

> 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.[9]

If the FAA does not heed its own warnings, the FAA will only have itself to blame when public backlash limits the opportunities for BVLOS operations.

THE FAA MUST IMPLEMENT TRANSPARENCY MEASURES AROUND BVLOS DRONE OPERATIONS

Transparency should be a fundamental element of BVLOS drone operations. This is a new technology. Its integration into our communities — the problems it will create and the side

---

[4] *Final Rule: Remote Identification of Unmanned Aircraft*, 86 Fed. Reg. 4390 (Jan. 15, 2021).
[5] Stolz, M., Papenfuss, A., de Albuquerque Richers, G.C. *et al.*, *A mixed-method approach to investigate the public acceptance of drones*. CEAS Aeronaut J 14, 835–855 (2023), https://doi.org/10.1007/s13272-023-00693-8.
[6] Min Zhou, Shuwei Yu, Chuting Zhou, Nan Kong, Kathryn S. Campy, *Navigating the future: A longitudinal exploration of public acceptance of autonomous taxis from initial trials to stepwise habituation*, Computers in Human Behavior, pp.108678 (2025), https://ieeexplore.ieee.org/abstract/document/10748821/.
[7] Ning Wang, Nico Mutzner, Karl Blanchet, *'We Need Time…': An Expert Survey on Societal Acceptance of Urban Drones*, Science and Public Policy, Volume 52, Issue 3,356–374 (June 2025), https://doi.org/10.1093/scipol/scae084.
[8] Hullysses Sabino, Rodrigo V.S. Almeida, *et al.*, *A systematic literature review on the main factors for public acceptance of drones*, Technology in Society 71 (2022), https://www.sciencedirect.com/science/article/abs/pii/S0160791X2200238X#preview-section-introduction.
[9] 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.

effects it may have — remain big unknowns. It is vital that the problems, successes, and failures be transparent so that the citizens of our democracy can make decisions about how it's working out, whether they want this technology overhead, and if so, what rules might need to be added or adjusted as the technology integrates into the complex physical and social spaces that make up our communities. Transparency allows the public and agencies to hold operators accountable and can also remove the mystery of drones and facilitate public acceptance. Transparency should extend to all aspects of drone operations that the public may have a stake in. That includes transparency around drone incidents (e.g. crashes and loss of control), Automated Data Service Providers (drone traffic routing) — to the extent they collect/use data that is considered personally identifiable — and drone operations, which should include, among other things, a drone's technical capabilities and what kind of data the drone may be collecting.

The FAA should also require a Privacy Impact Assessment (PIA) from operators as part of its process for granting permits and certificates for BVLOS operations. A PIA can serve not only as a way for drone operators to consider any potential privacy impact of their operations but also as a way for the public to be informed of the privacy risks of drone operations. Just as drone operators should understand the risks and potential impact that drone operations impose in terms of safety, noise, or environment, drone operators should also understand the potential privacy impact their operations may have. PIAs are a routine requirement for federal agencies and are increasingly used by companies to understand the privacy risks of their actions. A similar requirement should be required for all governmental and commercial BVLOS drone operations.

Doing such assessments, keeping them updated, and making them easily accessible to the public would go a long way in facilitating public acceptance of BVLOS drone operations, but only if the PIAs provide detailed and relevant information to the public. These assessments should include:

- **Type and purpose of the drone operation.** The operator should detail the purpose of its operation, so the public can understand its nature and hold them accountable for mission creep or privacy-invasive activities.
- **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, the document should specify 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.** Details 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.
- **Data use.** 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 shared, and for what purpose.
- **Analysis of privacy impact and any mitigation measures.** 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 mitigation measures are in place to address these issues.

Privacy impact assessments can go a long way in providing members of the public the transparency they need, but the public also should have access to real-time information about the drones in their vicinity. The best way to do that is with the Drone ID requirement.

THE FAA MUST UDPATE THE DRONE ID REQUIREMENT TO GIVE THE PUBLIC REALTIME TRANSPARENCY OF DRONE OPERATIONS HAPPENING NEAR THEM

The remote ID requirement is one of the best opportunities for the FAA to implement privacy-related rules that will facilitate transparency. 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 should let the public not only learn about what drones are flying near them, but also who is operating them, for what purpose, their surveillance capabilities, and the information the drone might be collecting.[10] This can be done directly through the information provided in the Remote ID signal or giving the public an easy means of accessing the privacy impact assessment that corresponds to each particular drone.

For the Remote ID requirement to mitigate the privacy risks of drones, the requirement must be useable and useful to the public. It should not be complicated for members of the 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. 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 FAA SHOULD IMPLEMENT MINIMIZATION REQUIREMENTS TO PREVENT SURREPTITIOUS DATA COLLECTION

It is not enough to simply provide transparency; it is important to ensure that the data collected is necessary for the purpose of the drone operation and prevent the broad collection of data for the sake of collecting data. Such data minimization is an important aspect of protecting privacy. Many of the suspicions and fears that surround drones come from the possibility that the aircraft are collecting information for purposes beyond what is necessary for their mission. Data minimization requirement serves other important purposes. First, it helps to prevent mission creep. If drones are used to constantly collect data on anything and everything in their vicinity while conducting drone operations, it is only a matter of time before that data is used for

[10] 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.

purposes unrelated to the core operation. Second, data minimization minimizes the impact of data breaches. Such breaches have become a frequent and widespread problem, affecting government agencies and even the largest and most well-funded companies. One way to counter data breaches is to minimize the data collected; you can't lose data you don't have.

A data minimization requirement would mandate that government and commercial BVLOS operators minimize the data collected, used, and shared to what's relevant and necessary to the operation of the drone and to carry out the purpose of the flight. For example, if a BVLOS drone is doing delivery, no data should be collected that is not strictly necessary to achieve that purpose, and data collected for that purpose should not be retained or used for other purposes. 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.

In order to protect the public, the FAA should, to the extent of its authorities, mandate, incentivize, or encourage a data minimization requirement, and urge Congress to enact such a requirement.

NEWSGATHERING MUST BE INCLUDED IN THE LIST OF PRIMARY BVLOS DRONE PURPOSES

The proposed rule states:

> Operating permits, proposed under subpart D of part 108, may be issued for eight possible purposes: package delivery, agriculture, aerial surveying, civic interest, operations training, demonstrations, recreational activity, and flight tests. [11]

One of the most important uses of drones is for newsgathering. For many years, newsgathering organizations have been one of the primary users of helicopter aviation, which allows such organizations to quickly roam across a city or county to gather news. As companies and government agencies turn to drones as a more cost-effective replacement for crewed helicopters, media organizations can be expected to want to do the same – including the full spectrum of newsgathering, reporting, and investigative organizations, including citizen journalists, who serve as checks and balances on corporate and government power. One of the promises of BVLOS operations is that it expands access to the national air space to those who can't afford a helicopter.

Under the proposed rule, newsgathering would be included within the category of "aerial surveying," which the agency defines as "operations conducted for the purposes of photography, videography, mapping, inspecting, or patrolling." In the Preamble the agency notes that "FAA anticipates that aerial surveying operations would occur in a multitude of population densities due to the various purposes of missions, such as newsgathering."[12]

[11] BVLOS NPRM at 38263-64.
[12] BVLOS NPRM at 38276.

We applaud the FAA for recognizing newsgathering within the universe of recognized BVLOS operations and strongly urge the agency to retain that recognition within the final rule. We also recommend that newsgathering be elevated to a primary use case along with the eight other use cases the agency proposes to recognize, given its central importance in a free society and the need for the FAA to more explicitly contemplate journalist uses of BVLOS flights. The agency must ensure that drone operations aren't dominated by commercial and government use, but serve all sectors of society including public interest groups and newsgathering organizations that provide important checks and balances on power in our society.

THE USE OF PRIVATE-SECTOR DATA SERVICE PROVIDERS REQUIRES STRONG RULES AROUND DATA ACCESS, DATA USE, AND IMPARTIALITY

The FAA seeks to accomplish a major public purpose — maintaining the safety of BVLOS flights — by requiring operators to do business with private companies charged with carrying out that function: what the agency calls Automated Data Service Providers. The FAA envisions that these Providers would provide "strategic deconfliction," for example — essentially, air traffic routing for drones, which in the world of legacy aviation is provided directly by the FAA itself.

Inserting private companies into such a key role in carrying out a public function raises questions about the companies that serve those roles and how they might exploit their role in the ecosystem.

First, the proposed rule does not address questions about access to data. As we discuss above, we believe that information about drone operations above communities should be available to members of the public. The agency envisions Automated Data Service Providers "exchanging information continuously with each other" in a peer network,[13] but the NPRM makes no provision to require that the information Automated Data Service Providers exchange in the course of providing services, such as deconfliction services, will be public. This raises the potential that companies participating in this network will have privileged access to nonpublic information about BVLOS drone operations — potentially even a global "bird's eye view" of all such operations. A database of BVLOS drone flights — from big companies making deliveries to photojournalists and scientists at work to recreational fliers — is not something to which private companies should have privileged access. If private Automated Data Service Providers gain access to such data, then it should also be provided to the public.

Second, in the proposed rules there does not appear to be any restrictions on how Providers might make use of such data, which would be vital if the data they access is not public. They might want to use that data for marketing, profiling, or market intelligence for example, and share data with anyone from immigration enforcement agencies to marketers and tabloid reporters.

Third, the proposed rules do not sufficiently address questions about giving decision-making power to private entities serving as Automated Data Service Providers. How much discretion in

[13] BVLOS NPRM at 38326-27.

the carrying out of activities such as strategic deconfliction will these Providers have in determining who may fly where, and when? Many or most of these Providers will presumably be for-profit companies, which may have many other business interests. Will they, if they are so inclined, be able to block a newsgathering BVLOS operation from aerial coverage of a protest, abusive police action," or union rally?

The FAA proposes an "impartiality" rule requiring that Providers "must provide their service to users in a reasonable and non-discriminatory manner, as applicable."[14] But if the fundamental incentive structure of the FAA's privatized traffic prioritization model does not place disinterested parties in the role of making these decisions, that language is not likely to be effective at ensuring impartiality. The motivations of some to be partial towards one party may be high and enforcement of impartiality will be difficult because it will often be hard to determine whether a particular decision was, in fact, motivated by political considerations, financial incentives, or otherwise discriminatory purposes. A biased party can always claim that operational considerations dictated their decision and that financial incentive or politics — or pleasing a law enforcement agency that would prefer not to have media cameras overhead — "had nothing to do with it."

We may anticipate situations where different parties want to engage in conflicting BVLOS operations: newsgathering organizations wanting to cover an event of public interest versus for-profit companies wanting to make deliveries; media versus law enforcement; unions versus employers.

The agency does say it "recognizes the need to establish a priority of operations schema" that would identify "priorities of operations" and guide service providers "on resolving conflicts when they exist among operators of the same priority level."[15] The agency says that schema is addressed in a draft advisory circular, AC 146-1. However, the bare-bones schema presented in that draft would still give for-profit Automated Data Service Providers vast discretion in making decisions of public importance about which BVLOS operations may operate at what place and time. The schema would also give law enforcement operations automated priority over all private operators. That is at a minimum too blunt of a rule given the history of abusive law enforcement attempts to block newsgatherers from recording their activities and the potential that some departments would intentionally exploit their priority to box out other users from air space.[16]

All of these issues would be intensified if the Provider marketplace undergoes concentration, as many markets naturally do, such that every BVLOS operator that is required by the FAA to use

[14] BVLOS NPRM at 38388, §146.300 (e).
[15] BVLOS NPRM at 38335.
[16] Faine Greenwood, "How to regulate police use of drones," Brookings Institute, Sept. 4, 2020, at https://www.brookings.edu/articles/how-to-regulate-police-use-of-drones/ (noting that "Police drones are a highly effective way for law enforcement to 'mark' the aerial territory over news-worthy events. While plenty of journalists and activists use drones to collect their own aerial information, they're often reluctant to fly when there's a chance they could be accused of interfering with a drone or a helicopter operated by police."). See also Jay Stanley, "Curbs Needed on Police Drone Surveillance of Public Gatherings," American Civil Liberties Union, March 14, 2024, at https://www.aclu.org/wp-content/uploads/2024/03/Curbs-Needed-On-Police-Drone-Surveillance-of-Public-Gatherings-FINAL-2.pdf#page=7.

an Automated Data Service Provider in order to fly is forced to do business with one or two large companies.

The FAA does allow BVLOS operators to serve as their own Automated Data Service Providers, which might ameliorate some of these issues. Serving that role, however, subjects an operator to all of the Part 146 regulations in addition to the Part 108 regulations, and it's not clear how many operators, especially small operators, will be able, as a practical matter, do so this.

Inserting private companies into the middle of a governmental infrastructure for the regulation of drone flights raises questions about how such a regulatory role will interact with the profit motives and other incentives to which for-profit companies are subject. If that is to be done, it should be done with a recognition of the potential ways that moneyed interests might exploit that position, and with strong checks and balances to prevent such exploitation. Those appear to be absent in the current proposal.

LOCAL COMMUNITIES MUST HAVE INPUT ON BVLOS OPERATIONS IN THEIR NEIGHBORHOODS

The proposed rules contain no provisions for local community input into BVLOS operations in the skies over their streets and homes. In a democracy, it's important that communities have a say over how this technology affects them. One of our biggest concerns is that an FAA BVLOS regulation will allow large companies and other parties with no connections to a local community to operate in that community against the wishes of residents and will leave no room for addressing privacy and other problems or concerns that emerge.

We do not yet know whether American communities want drones in their lives — whether they will accept regular or frequent flights, and if so under what conditions. That will depend on a 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, nuisance, privacy invasiveness, and value. As discussed above, there is plenty of evidence that many people feel very uneasy about the technology.

The fact is, if drones were invented before crewed aircraft, they would almost certainly be regulated locally, like electric scooters. Airliners and other crewed aviation require a uniform set of rules across the entire country; modern aviation obviously wouldn't be possible if every county could set their own rules for crewed aircraft passing overhead. With drones, on the other hand, if one state or locality bans them or imposes stringent regulations, that generally does not affect other states or localities. That is certainly true for non-BVLOS Part 107 operations, but even BVLOS flights will generally likely only range so far.

If fully exercised, the FAA's legacy authority to exclusively regulate drones at the national level threatens to short-circuit the normal political give-and-take that occurs among local stakeholders when any disruptive new technology is introduced into communities. The advent of technologies like cars, bicycles, electric scooters, leaf blowers, ridesharing services — even skateboards — have stirred up local controversy throughout history, and drones are likely to do the same.

From its perch in Washington DC, the FAA should not try to anticipate how communities will react to drones in the coming years and decades, what local problems they will create, and what kinds of restrictions, regulations, or compromises will solve the conflicts to their satisfaction.

Most Americans haven't yet given much thought to drones. Other than a few hobbyists, most of those who are thinking about the technology today represent law enforcement or industry. But a by-right regime of noisy and camera-carrying corporate flying robots forced on communities will likely leave many of them feeling helpless and angry. The anger long sparked in some communities by airport noise may emerge in every small neighborhood across the nation. When residents feel there is too much wheeled vehicle traffic by 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.

We don't want to see drones imposed on unwilling communities in disruptive and inequitable ways, 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). The FAA should voluntarily forbear assertion of its legal right to regulate the NAS and allow localities to restrict or entirely ban drone operations in their jurisdictions, seeking authorization from Congress to do so if necessary. 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.

FAA AND TSA SHOULD NOT BUILD UPON A FLAWED BACKGROUND CHECK SYSTEM

The FAA proposes to require certain staff involved in BVLOS operations undergo a Level 3 security threat assessment by the Transportation Security Agency, which, as the NPRM notes, includes "a check of criminal history, immigration, and intelligence-related databases and watchlists." Under 49 CFR § 1572.107 the TSA may reject an applicant based on a conviction for any "serious crime" or based on a search of "Terrorist watchlists and related databases or "any other databases relevant" to whether someone is "suspected of posing" a security threat.

We agree that BVLOS drones pose a potential security threat, and that operators of such drones, like others who work in aviation roles that pose similar risks, should be subject to reasonable security measures proportional to that threat. But the TSA's threat assessment process is deeply flawed, irrational, and unfair, and should not be extended to exclude workers from participation in BVLOS operations.

Denying those with a criminal record from working in the BVLOS field often does not make sense. The criminal justice system is highly discriminatory. Black people, for example, are more likely to be targeted across the range of criminal justice interventions, from stops, searches, and

arrests, to prosecutions, convictions, and sentencing. This is among the reasons that the "ban the box" social movement has arisen to stop the lifetime employment blacklisting of those unfairly caught up in the criminal justice system or who made mistakes in their life and have served their sentences. There is no rational reason, for example, why someone convicted in their youth of "possession of a controlled substance with intent to distribute" [49 CFR § 1572.103 (b)(2)(vii)] should be barred from working with BVLOS drones.

The use watchlist checks is also deeply problematic. The government exercises virtually unfettered discretion in deciding whom to place on the nation's secretive watchlisting system. The full extent of how and why individuals are placed on the master terrorism watchlist has never been publicly revealed, but we know the criteria are extremely vague. The placement criteria for the No Fly List, for example, say merely that there must be "reasonable suspicion" that a person "poses a threat" of committing terrorism, with these terms only vaguely defined ("reasonable suspicion" here being distinct from, and more vague than, the legal Fourth Amendment standard for that term).[17]

Indeed, in litigation the government has made plain that the threshold is very low for a potential lifetime ban on the right to travel. Uncorroborated and even doubtfully reliable information is enough to land an individual on the watchlist, and, according to the National Counterterrorism Center, "concrete facts are not necessary."[18] Placement on a watchlist does not require "any evidence that the person engaged in criminal activity, committed a crime, or will commit a crime in the future."[19] Something as innocuous as "an individual's travel history" or course of "study of Arabic" suffices to support a nomination onto the No Fly List.[20]

These loose, amorphous, and shifting standards increase the likelihood that the No Fly List—and indeed the watchlisting system as a whole—includes people who are entirely innocent of past, present, and future criminal wrongdoing. The FAA should not increase reliance on this illegitimate system by including it in the BVLOS security procedures.

[17] Overview of the U.S. Government's Watchlisting Process and Procedures at 2, *Elhady v. Kable*, No. 16-cv-375 (E.D. Va. Mar. 12, 2019), ECF No. 308-12.
[18] National Counterterrorism Center, Watchlisting Guidance (2013) at 70, https://www.aclu.org/sites/default/files/field_document/March%202013%20Watchlist%20Guidance.pdf.
[19] *Elhady v. Kable*, 391 F. Supp. 3d 562, 569 (E.D. Va. 2019), *rev'd and remanded*, 993 F.3d 208 (4th Cir. 2021) (internal quotation marks omitted).
[20] *Id.*