United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued December 15, 2021 Decided July 29, 2022

No. 21-1087

TYLER BRENNAN AND RACEDAYQUADS LLC,
PETITIONERS

v.

STEPHEN DICKSON, ADMINISTRATOR AND FEDERAL AVIATION ADMINISTRATION,
RESPONDENTS

On Petition for Review of an Order
of the Federal Aviation Administration

Jonathan Rupprecht argued the cause for petitioners. With him on the briefs were *Elizabeth Candelario* and *Kathleen Yodice*.

Casen B. Ross, Attorney, U.S. Department of Justice, argued the cause for respondents. With him on the brief were *Brian M. Boynton*, Acting Assistant Attorney General, *Michael S. Raab*, Attorney, *John E. Putnam*, Acting General Counsel, U.S. Department of Transportation, *Paul M. Geier*, Assistant General Counsel, and *Charles E. Enloe*, Trial Attorney.

Joshua S. Turner and *Sara M. Baxenberg* were on the brief for *amicus curiae* the Association for Unmanned Vehicle Systems International in support of respondents.

Before: PILLARD, WILKINS and WALKER, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* PILLARD.

PILLARD, *Circuit Judge*: Drones are coming. Lots of them. They are fun and useful. But their ability to pry, spy, crash, and drop things poses real risks. Free-for-all drone use threatens air traffic, people and things on the ground, and even national security. Congress recognizes as much. It passed a law in 2016 requiring the Federal Aviation Administration (FAA) to "develop[] . . . consensus standards for remotely identifying operators and owners of unmanned aircraft systems" and to "issue regulations or guidance, as appropriate, based on any standards developed." FAA Extension, Safety, and Security Act of 2016 (FAA Extension Act), Pub. L. No. 114-190, § 2202(a), (d), 130 Stat. 615, 629 (2016). And in 2018, Congress extended the FAA's authority over small recreational drones. FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 349(f)(3), 132 Stat. 3186, 3299 (2018). In response to Congress's call to prioritize the development of capacities to increase airspace awareness and promptly mitigate threats as a means to protect the safety and security of U.S. airspace, the FAA promulgated the Remote Identification (Remote ID) Rule challenged here.

Remote ID technology requires drones in flight to emit publicly readable radio signals reflecting certain identifying information, including their serial number, location, and performance information. Those signals can be received, and the Remote ID information read, by smart phones and similar devices using a downloadable application available to the

FAA, government entities, and members of the public, including other aircraft operators. The FAA likens Remote ID to a "digital license plate." Remote Identification of Unmanned Aircraft (Final Rule or Remote ID Rule), 86 Fed. Reg. 4390, 4396 (Jan. 15, 2021); FAA Br. at 17. Like a license plate, Remote ID acts as a basic building block of regulatory compliance by attaching a unique, visible, yet generally anonymous identifier to each device in public circulation. Unlike a license plate on the back of a car, however, Remote ID is detectible in real time only when the drone is moving. Also unlike a vehicle's license plate, which can only be read by the naked eye from a few yards away, a Remote ID message can be "read" by people within range of local radio signals yet not near enough even to see the drone itself.

The FAA separately obtains certain nonpublic personally identifying information from drone owners as a requisite of their unmanned aircraft registrations, and that information is protected by the Privacy Act, 5 U.S.C. § 552a. A Remote ID message may only be matched to that nonpublic information and used by the FAA or disclosed to law enforcement outside of the FAA "when necessary and relevant to a[n] FAA enforcement activity," Privacy Act of 1974; System of Records Notice, 81 Fed. Reg. 54,187, 54,189 (Aug. 15, 2016), and even then it is subject to "all due process and other legal and constitutional requirements," Final Rule, 86 Fed. Reg. at 4433. The Rule does not otherwise authorize private or public actors access to drone owners' or pilots' nonpublic personally identifying information, *id.* at 4433-34, nor does it permit or contemplate storage of Remote ID data for subsequent record searches.

Petitioners Tyler Brennan, a drone user, and RaceDayQuads, the drone retailer Brennan owns (referred to jointly as Brennan), want the Rule vacated. Brennan asserts

that the Rule's Remote ID requirement amounts to constant, warrantless governmental surveillance in violation of the Fourth Amendment. His request for vacatur of the Rule, amounting to a facial challenge, must fail because drones are virtually always flown in public. Requiring a drone to show its location and that of its operator while the drone is aloft in the open air violates no reasonable expectation of privacy. Brennan hypothesizes that law enforcement authorities could use Remote ID to carry out continuous surveillance of drone pilots' public locations amounting to a constitutionally cognizable search, or that the Rule could be applied in ways that would reveal an operator's identity and location at a home or in an otherwise private place. But he has not shown that any such uses of Remote ID have either harmed him or imminently will do so, thus he presents no currently justiciable, as-applied challenge.

Brennan also claims that the Remote ID Rule must be vacated due to various procedural missteps he believes the FAA made in promulgating it. But none of those asserted flaws affects the validity of the Rule. The communications that Brennan challenges as *ex parte* did not materially bear on the rulemaking, so their exclusion from the administrative record did not interfere with the requisite opportunity for public comment. The Final Rule's provisions for altitude measurement using geometric pressure and retrofitting of existing unmanned aircraft equipment are logical outgrowths of the Proposed Rule on which the public was able to—and did—comment. The FAA also fulfilled the statutory directive that it consult with the Radio Technical Commission for Aeronautics, Inc. (RTCA), the National Institute of Standards and Technology (NIST), and industry stakeholders. Finally, Brennan faults the FAA for not adequately addressing certain comments, but the FAA need not respond to purely speculative comments, and its consideration of about 53,000 public

comments and detailed explanation of the policy choices in the Final Rule fully met its obligation under the Administrative Procedure Act (APA).

We accordingly deny the petition.

BACKGROUND

I. Factual context of the Final Rule

The Remote ID Rule responds to the development of sophisticated yet inexpensive drone equipment, which "has allowed for hundreds of thousands of new operators to enter the aviation community." Final Rule, 86 Fed. Reg. at 4395. Drones' growing accessibility has unlocked a large recreational market for both factory- and home-made models: Of the 865,505 drones registered with the FAA by mid-2022, 538,172 were for recreational use. *See Drones by the Numbers*, FAA (May 31, 2022), https://www.faa.gov/uas/resources/by_the_numbers/. Meanwhile, rapidly accelerating commercial uses and planned uses of drones include infrastructure inspection, real estate photography, and agriculture management. Universities use them for research activities. The healthcare industry uses drones to deliver medical supplies, whether to quickly traverse high-congestion cities or to reach remote areas lacking other viable transport. Governments at every level increasingly rely on drones' distinctive capabilities for tasks ranging from search-and-rescue missions to border patrol. Public and private emergency responders alike use drones to observe hard-to-reach accident sites, monitor natural disasters, and assist in rescue and recovery. *See* Amicus Br. of the Ass'n for Unmanned Vehicle Sys. Int'l at 5. And plans are afoot for major expansions of other, routine drone uses such as express

package shipping and delivery. *E.g.*, Final Rule, 86 Fed. Reg. at 4481.

All the while, increasing drone usage creates more air traffic. And the features that make drones so popular present novel and complex challenges to a smooth integration of drones into the 29 million square miles of U.S. airspace that tens of thousands of commercial and private aircraft share each day. Congestion increases risks of drone collisions with other aircraft, especially helicopters or agricultural aircraft flying at low altitudes, and aircraft taking off or landing at airports, landing strips, or heliports. The established U.S. air traffic control system depends on constant lines of communication between traffic controllers and pilots in flight to avert risks to aircraft and to people and property on the ground. But drones have no operator on board to receive or transmit air-traffic communications, nor do they communicate with a centralized FAA tower to coordinate with nearby aircraft. Without Remote ID, pilots must rely solely on visual inspection of the sky to avoid collisions with drones, and manned aircraft are likewise left without electronic data on the locations of any drones flying in their vicinity. Drones' technical capability of flying at night, over people, and beyond their operators' lines of sight pose additional risks associated with a lack of situational awareness, including collision with other aircraft or objects, falling on and injuring people, and straying into private or sensitive areas. Safety concerns pertaining to national security and law enforcement are intensified when unidentified drones of unknown origin and intent fly over airports, public facilities, energy production infrastructure, sports stadiums, or other open-air venues where the concentration of people is high or the ability to damage things and disrupt daily life is significant. *See, e.g.*, Remote Identification of Unmanned Aircraft Systems

(Proposed Rule), 84 Fed. Reg. 72,438, 72,455 & nn.22, 26 (proposed Dec. 31, 2019). [1]

Drones in flight are also difficult to identify with the naked eye. Prior regulations required the exterior of all small drones flown in U.S. airspace to be marked with the device's registration number. *See* 14 C.F.R. §§ 48.200, 48.205 (2021). But a number physically marked on a drone itself "is only visible upon close inspection, making visual identification of unmanned aircraft in flight difficult or impossible." Final Rule, 86 Fed. Reg. at 4397. The known difficulty of identifying drones from afar increases the likelihood that drone operators will engage in reckless, prying, or aggressive behavior under cover of anonymity. Unseen and potentially untraceable operators may fly drones in uncoordinated, intrusive, or unsafe ways.

Errant drone flights are not unusual: In 2019, the FAA alone received an average of six reports daily from people who claimed to have witnessed unauthorized drone operations. Proposed Rule, 84 Fed. Reg. at 72,455. The FAA has noted the potential use of drones for illegal activities, including "carrying and smuggling of controlled substances, illicit drugs, and other dangerous or hazardous payloads; the unlawful invasion of privacy; illegal surveillance and reconnaissance; the weaponization of [drones]; sabotaging of critical

---

[1] Citing Scott Gleeson, *Juvenile Was Operating the Drone that Flew Over Fenway Park in Red Sox Game, Police Say*, USA TODAY (Apr. 13, 2019), https://www.usatoday.com/story/sports/mlb/redsox/2019/04/13/drone-fenway-park-juvenile/3457190002/; Lori Aratani, *Drone Activity Halts Air Traffic at Newark Liberty International Airport*, WASH. POST (Jan. 22, 2019), https://www.washingtonpost.com/transportation/2019/01/22/drone-activity-halts-air-traffic-newark-liberty-international-airport/.

infrastructure; property theft; disruption; and harassment." *Id.* at 72,454. Extremists have increasingly sought to use drones to carry out violent attacks: Terrorists killed several people by detonating a bomb carried by a drone that flew above a military parade in Yemen. *Id.* at 72,455 & n.34.[2] The Islamic State and other terrorist organizations have reportedly modified commercially available drones so they can carry and release munitions and explosives. *Id.* at 72,455 & n.31.[3] A would-be assassin used a drone to target then-President Nicolás Maduro in Venezuela. *Id.* at 72,455 & n.32.[4] And British intelligence agencies uncovered a terrorist plan to fly drones into the engines of commercial airplanes as they took off from airports in the United Kingdom. *Id.* at 72,455 & n.33.[5]

II. Legal context of the Final Rule

Congress has responded to the rapid proliferation of drones, and the unique challenges they pose, by enacting laws to guide a safe and efficient transition to a new chapter in U.S. airspace use. It defined an "unmanned aircraft," or drone, as

---

[2] Citing *Houthi Drones Kill Several at Yemeni Military Parade*, REUTERS (Jan. 10, 2019), https://www.reuters.com/article/us-yemen-security/houthi-drones-kill-several-at-yemei-military-parade-idUSKCN1P40N9.

[3] Citing Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats*, COMBATING TERRORISM CTR. AT WEST POINT, at iv (July 2018), https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.

[4] Citing *Venezuela President Maduro Survives 'Drone Assassination Attempt'*, BBC (Aug. 5, 2018), https://www.bbc.com/news/world-latin-america-45073385.

[5] Citing Patrick Williams, *Terror Drone Plot FOILED: Brit Spies Stop Plan to Bring Down AIRLINER*, DAILY STAR (Aug. 19, 2018), https://www.dailystar.co.uk/news/latest-news/terror-drone-plot-britain-uk-16886096.

"an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft," 49 U.S.C. § 44801(11), plus the aircraft's system of "associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system," *id.* § 44801(12).

The United States Government "has exclusive sovereignty of airspace of the United States," and the FAA is congressionally empowered to "develop plans and policy for the use of the navigable airspace and assign by regulation or order the use of the airspace necessary to ensure the safety of aircraft and the efficient use of airspace." *Id.* § 40103(a)(1), (b)(1). The navigable airspace of the United States includes airspace above minimum flight altitudes and the airspace necessary for safe takeoff and landing of aircraft. *Id.* § 40102(a)(32). Federal law calls on the FAA to

> prescribe air traffic regulations on the flight of aircraft (including regulations on safe altitudes) for—
>
> (A) navigating, protecting, and identifying aircraft;
>
> (B) protecting individuals and property on the ground;
>
> (C) using the navigable airspace efficiently; and
>
> (D) preventing collision between aircraft, between aircraft and land or water vehicles, and between aircraft and airborne objects.

Id. § 40103(b)(2). The agency must also "promote safe flight of civil aircraft in air commerce by prescribing . . . regulations and minimum standards for other practices, methods, and procedure the Administrator finds necessary for safety in air commerce and national security." *Id*. § 44701(a), (a)(5).

In late 2011, Congress directed the FAA to establish drone test sites, *see* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 1097, 125 Stat. 1298, 1608-09 (2011) (codified at 49 U.S.C. § 40101 note), and in 2012 it called on the FAA to create a system to regulate the operation of small civil (*i.e.* nongovernmental) drones to integrate them into national airspace, *see* FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, §§ 332, 333, 126 Stat. 11, 73-76 (2012). The FAA then promulgated a comprehensive set of regulations for routine use of small, unmanned aircraft in 2016. 14 C.F.R. pt. 107. At first, Congress expressly excluded model aircraft, or small drones used strictly for hobby or recreational use, from its call for drone regulation. *See* FAA Modernization and Reform Act, § 336(a), 126 Stat. at 77 (providing that the FAA "may not promulgate any rule or regulation regarding a model aircraft"); *Taylor v. Huerta*, 856 F.3d 1089, 1092 (D.C. Cir. 2017).

But rapidly increasing drone use and the associated complexities prompted further congressional action, laying the foundation for the rule at issue here: The FAA Extension Act of 2016 directed the FAA to develop the capacity to remotely locate drones in flight and contact their operators as needed to ensure regulatory compliance. *See* FAA Extension Act, § 2202(a), 130 Stat. at 629. In particular, the Act required the FAA to report to the relevant congressional committee on any remote identification standards developed within one year of the Act, and then issue appropriate regulations or guidance no later than one year after the report. *Id.* § 2202(c)-(d), 130 Stat.

at 629. And in the FAA Reauthorization Act of 2018, Congress tightly curtailed the statutory exception for small hobbyist drones and made clear that they are generally subject to the same rules regarding registration and marking, remote identification, and "maintaining the safety and security of the national airspace system" as applied to other unmanned aircraft and unmanned aircraft systems. FAA Reauthorization Act, § 349(a), (b), (f), 132 Stat. at 3297; 49 U.S.C. § 44809(f); *see* Final Rule, 86 Fed. Reg. at 4403.

III. The Remote ID Rule

The FAA complied with Congress's call for a regulatory system of remote identification of drones and their pilots by promulgating the Remote ID Rule in January 2021. By developing a general requirement that drones be capable of Remote ID, the FAA aimed to "provide airspace awareness to the FAA, national security agencies, law enforcement entities, and other government officials." Final Rule, 86 Fed. Reg. at 4393. In the face of increasing drone use in U.S. airspace, the FAA sought a means "to distinguish compliant airspace users from those potentially posing a safety or security risk." *Id.* at 4395; *accord* FAA Br. at 7.

Remote ID promises "greater situational awareness of [drone] operations to airport operators and other aircraft in the vicinity of those operations" that enables the FAA to safely accommodate drone flight together with low-altitude flight of manned aircraft. Final Rule, 86 Fed. Reg. at 4488. The FAA predicted that near-real-time Remote ID would "enhance threat assessments" and "discourage[] unsafe flying by operators of unmanned aircraft, thereby promoting safety for other users of the airspace of the United States and for those on the ground." *Id.* at 4490. According to the FAA, the Remote ID Rule advances its mission to "promot[e] the safe and efficient use of

the navigable airspace" by "strengthen[ing] the FAA's oversight of [drone] operations and support[ing] efforts of law enforcement to address and mitigate disruptive behavior and hazards, which may threaten the safety and security of [U.S.] airspace." *Id.* at 4493. Identifying drone operators "enable[s] better threat discrimination, an immediate and appropriate law enforcement response, and a more effective follow-on investigation." *Id.* at 4435.

The Remote ID Rule is the product of a year-long public rulemaking in which the agency received approximately 53,000 comments. *See* Proposed Rule, 84 Fed. Reg. 72,438 (proposed Dec. 31, 2019). Its Remote ID requirement becomes effective on September 16, 2023, Final Rule, 86 Fed. Reg. at 4390, and it requires nonmilitary drones weighing over 0.55 pounds and registered with the FAA to signal identifying information during flight, *id.* at 4403, 4505. Drones subject to the Rule must use unlicensed, publicly accessible local radio frequencies and remain in compliance with the Remote ID requirements. The Rule does not allow disabling of Remote ID functions, and if a drone experiences Remote ID failure or malfunction, its operator must land the device as soon as practicable.

Drones must emit the Remote ID signal while the drone is in flight, from its takeoff to shutdown; the requirement is inapplicable while the drone is "entirely indoors, underground, or inside an enclosed space such as a netted enclosure." *Id.* at 4404. All broadcasts are local and use unlicensed radio frequency spectrum that smart devices, like smart phones, tablets, or similar commercially available devices, can receive "within a limited proximity." *Id.* at 4428. The FAA and anyone with the proper equipment nearby will be able to receive those signals in real time during the drone's flight. The Rule "does not contemplate the FAA's routine collection or

retention of broadcast information. At this time, the FAA does not have plans to collect or retain the broadcast information." U.S. DEP'T OF TRANSP., PRIVACY IMPACT STATEMENT – FAA, REMOTE IDENTIFICATION OF UNMANNED AIRCRAFT FINAL RULE at 10 (2021), J.A. 221.

The Rule specifies three categories of Rule-compliant drones based on their Remote ID capabilities. Standard Remote ID drones are commercially manufactured drones, which, as of September 16, 2022, must be designed and produced to emit radio signals directly from the drone in flight. Broadcast Module drones are those built before September 16, 2022, without Remote ID capacity, which are retrofitted with a module to enable that capacity in compliance with the Rule; once modified, they may only be flown within the operator's line of sight. Unidentified drones without any Remote ID capability may only fly within the drone pilot's sight within FAA-recognized identification areas, or ID Areas—specific geographic areas set aside by the FAA for recreational or educational drone flight. Community-based organizations and educational institutions, including primary and secondary schools, trade schools, colleges, and universities, may apply to the FAA for ID-Area status.

A Standard Remote ID drone in flight must continuously emit: (1) its unique identification number; (2) its latitude, longitude, geometric altitude, and velocity; (3) the latitude, longitude, and geometric altitude of the drone's control station; (4) a time mark; and (5) any applicable "emergency status" indication (downed aircraft, low fuel, low battery, or other abnormal drone status not apparent from the nonemergency information or the drone's appearance). Final Rule, 86 Fed. Reg. at 4410, 4412, 4423. Retrofitted Broadcast Module drones must generally share the same information, except that, in keeping with reasonable limits on retrofit technology, they

only need identify the drone's takeoff location, not its control center's location throughout the drone's flight nor its emergency status.

The unique identification number referenced by the Rule is the drone's serial number. A drone owner must register the serial number with the FAA, along with the owner's name and contact information, to enable the FAA to identify and contact owners and hold them personally accountable for their aircraft. *See* 14 C.F.R. § 48.110 (required drone registration data); *id.* § 48.15 (requirement to register drones); *see also* 49 U.S.C. § 44102 (aircraft registration requirements). But serial numbers are not generally available to the public. Access to owners' personally identifying information contained in FAA registration records is "strictly limited to authorized FAA and other government and law enforcement personnel who are operating in their official capacities pursuant to all legal limitations and authorized use of the information," including legal and constitutional requirements. Final Rule, 86 Fed. Reg. at 4433. Federal, state, and local law enforcement personnel, like any member of the general public, can receive Remote ID messages, but the Rule does not authorize anyone other than personnel engaged in FAA enforcement activity to access individuals' drone registration data. *See* FAA Br. at 12-13, 31 n.4. While the Rule refers to potential future uses of Remote ID information by law enforcement, the FAA has not addressed the circumstances under which accredited and verified law enforcement personnel and federal agencies might access drone operators' identifying information, other than to reiterate that legal and constitutional limits would apply.

IV. The petition for review

Tyler Brennan is an Air Force pilot and self-proclaimed "avid drone user." Pet. Br. at 16. He describes his company,

RaceDayQuads, as a "one stop drone shop" that sells drones and drone parts and offers technical support. RACEDAYQUADS, https://www.racedayquads.com/ (last visited July 26, 2022). RaceDayQuads, says Brennan, has served more than 40,000 different customers per year in its almost four years of existence. Again, for convenience we jointly refer to owner and company as Brennan.

Brennan seeks review and vacatur of the Final Rule. He argues that the location tracking required by the Remote ID Rule infringes a drone operator's reasonable expectation of privacy so constitutes a warrantless search in violation of the Fourth Amendment. He also claims that the Final Rule is arbitrary and capricious on four grounds: (1) the FAA impermissibly relied on *ex parte* communications during the rulemaking that were not in the administrative record nor available for public comment; (2) aspects of the Final Rule were not logical outgrowths of the Proposed Rule; (3) the FAA failed to comply with a statutory requirement to consult with specified entities in formulating standards; and (4) the FAA failed to address material comments. The petition is timely and 49 U.S.C. § 46110(a) grants us jurisdiction to review.

DISCUSSION

As every pilot knows, Congress has authorized the Federal Aviation Administration to regulate the public airspace of the United States. FAA regulation enables safe and efficient shared use of the skies by government, commercial aviation, and private pilots. Most existing aviation rules are inapplicable to drones, but the Rule at issue here is specially fashioned at the behest of Congress to ensure that even drone pilots shoulder the baseline responsibility of reciprocal airspace awareness: At a minimum, drone pilots must enable other pilots and people on the ground who may be affected by their drones to discern

their location during flight. Remote ID provides that direct link between the drone and its pilot and enables accountability of drone pilots analogous to that of pilots collocated with manned aircraft. Final Rule, 86 Fed. Reg. at 4419. For the following reasons, we conclude that Brennan has failed to show that the Remote ID Rule violates the Fourth Amendment, and that his procedural challenges likewise lack merit.

I. Fourth Amendment claim

It is hard to see what could be private about flying a drone in the open air. Activities that require privacy are not typically conducted aloft; in contrast to how we use our homes, cars, and cell phones, people do not ordinarily live in or store private objects or information in their drones. Rather, as with cars traveling on public streets and highways or helicopters taking off, drones that take to the skies ordinarily make themselves visible to onlookers. And a drone pilot who elects to fly outdoors puts an aircraft into airspace used by rapidly increasing numbers of other new users—both other aircraft piloted remotely and myriad aircraft taking off or landing with pilots aboard.

Brennan claims that the Rule interferes with his reasonable expectation of privacy without requiring a warrant, in violation of the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. His briefing highlights certain potential applications of the Rule: "To be clear," he acknowledges, "Remote ID for recreational drones is **very** much appropriate when tied to legitimate safety and security concerns." Pet. Br. at 20 (emphasis in original). But this Rule, Brennan asserts, was promulgated not to protect airspace safety but to enable the government to conduct "intrusive tracking of everyone, everywhere, all the time, with extremely low costs

and ease of accessibility for law enforcement without judicial safeguards." *Id*. at 30. Citing the Supreme Court's Fourth Amendment precedent on electronic searches by law enforcement, Brennan argues that the Remote ID Rule matches or exceeds the intrusions those cases disapproved. *Id.* at 27-30 (citing *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018), *Riley v. California*, 573 U.S. 373, 385 (2014), and *United States v. Jones*, 565 U.S. 400, 403 (2012); *id.* at 416 (Sotomayor, J., concurring)). Brennan also underscores the special Fourth Amendment solicitude for the privacy of the home and its curtilage, which he says the Rule invades because drones may be "flown close to the ground and hidden from view by vegetation and fences in a private backyard." Pet. Reply Br. at 5; *see id*. at 12-13 (citing *Kyllo v. United States*, 533 U.S. 27, 33 (2001)); Pet. Br. at 22-25 (citing *Collins v. Virginia*, 138 S. Ct. 1663 (2018)).

The FAA responds that the Remote ID Rule does not invade any reasonable expectation of privacy, both because aviation is extensively regulated and because the Rule applies only to drone flights outdoors. FAA Br. at 23-34. By the same token that identifying the airborne location of an aircraft and collocated pilot with a transponder is not a Fourth Amendment search, the FAA says, using Remote ID to learn the locations of airborne drones and their pilots invades no constitutionally recognized privacy interest. *Id*. at 23-24 (citing *United States v. Bruneau*, 594 F.2d 1190, 1197 (8th Cir. 1979)). Even if the Rule did implicate constitutional privacy, the FAA contends that the searches it contemplates are excepted from the Fourth Amendment's warrant requirement. FAA Br. at 21-37; *see also Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (special needs search); *New York v. Burger*, 482 U.S. 691, 712 (1987) (administrative search of "closely regulated" business).

Brennan's pre-enforcement Fourth Amendment claim seeks wholesale vacatur of the Remote ID Rule, Pet. Br. at 20, 65, so we understand him to be challenging the Rule's facial validity—an unusual but not unheard-of type of Fourth Amendment claim. *See City of Los Angeles v. Patel*, 576 U.S. 409, 415-16 (2015) (citing cases). To prevail, Brennan "must establish that no set of circumstances exists under which the [rule] would be valid." *Ass'n of Priv. Sector Colls. & Univs. v. Duncan*, 681 F.3d 427, 442 (D.C. Cir. 2012); *accord United States v. Salerno*, 481 U.S. 739, 745 (1987). Identifying potential applications of the rule that could be unlawful is not enough. *Sherley v. Sebelius*, 644 F.3d 388, 397 (D.C. Cir. 2011). And because "[v]irtually *every* legal (or other) rule has imperfect applications in particular circumstances," *Barnhart v. Thomas*, 540 U.S. 20, 29 (2003) (emphasis in original), we need not—indeed, cannot—"resolve every hypothetical presented" by Brennan, *Nat'l Ass'n of Reg. Util Comm'rs v. FERC*, 964 F.3d 1177, 1188 (D.C. Cir. 2020); *see also Am. Bankers Ass'n v. Nat'l Credit Union Admin.*, 934 F.3d 649, 667-68 (D.C. Cir. 2019). Where a challenged rule does not exceed statutory authority and comports with the APA, "we will uphold the provision and preserve the right of complainants to bring as-applied challenges against any alleged unlawful applications." *Ass'n of Priv. Sector Colls. & Univs.*, 681 F.3d at 442.

Brennan's facial Fourth Amendment challenge fails because drone pilots generally lack any reasonable expectation of privacy in the location of their drone systems during flight. A "search" for purposes of the Fourth Amendment occurs when government action infringes a sphere an individual seeks to preserve as private and the expectation of privacy is one society considers reasonable under the circumstances. *Carpenter*, 138 S. Ct. at 2213; *Smith v. Maryland*, 442 U.S. 735, 740 (1979); *Katz v. United States*, 389 U.S. 347, 361

(1967) (Harlan, J., concurring). Brennan does not dispute the general visibility to onlookers of drones in the sky. Drones fly in the open, and people ordinarily lack a reasonable expectation of privacy "for activities conducted out of doors in fields." *Oliver v. United States*, 466 U.S. 170, 178 (1984). "[O]pen fields beyond the curtilage of a home, whether or not privately owned, are not among the protected places and things enumerated in the [Fourth] Amendment's text, so they fall outside the Fourth Amendment's coverage." *N. Am. Butterfly Ass'n v. Wolf*, 977 F.3d 1244, 1264 (D.C. Cir. 2020) (discussing *Oliver*, 466 U.S. at 176-80) (formatting modified). And there is no reasonable expectation of privacy in the movement of objects outside a residence where they can be viewed from a public route or adjoining premises, *United States v. Knotts*, 460 U.S. 276, 281-82 (1983), nor in activities conducted in the curtilage of a home, even behind a hedge or fence, if they may be viewed by "naked-eye observation" from an "aircraft lawfully operating" above the property, *California v. Ciraolo*, 476 U.S. 207, 213 (1986).

Brennan suggests pilots might use a drone's control station inside a home or fly the drone in its curtilage below the treeline out of public view. But the Rule does not mandate Remote ID for drone flights indoors, thus exempting flights inside a home, barn, or other private building. *See* Final Rule, 86 Fed. Reg. at 4404. Nor does it require Remote ID for drone flights in netted outdoor enclosures. *Id*. And nothing in the administrative record establishes that drones covered by the Remote ID Rule are usually flown from or in private spaces not visible to others, making drone systems' potential uses there no basis for facial invalidation.

Sometimes government surveillance of conduct that takes place in public can nonetheless run afoul of the Fourth Amendment, *see, e.g.*, *Carpenter*, 138 S. Ct. at 2217; *Jones*,

565 U.S. at 405, but the Remote ID Rule does not authorize any such privacy-invading practice. That is so for at least three interrelated reasons.

First, the Rule calls for installation, not monitoring by law enforcement. Owners of existing drones who fly outdoors and beyond approved drone-recreation areas (ID Areas) must retrofit their equipment with Remote ID broadcast modules and, as of September 2022, commercially produced drones must be equipped with Remote ID. *See* 86 Fed. Reg. at 4410-11. Brennan does not assert that equipping unmanned aircraft with Remote ID capability is itself a search in violation of the Fourth Amendment. And rightly so, as the installation of a device capable of location tracking merely creates the "potential for an invasion of privacy." *United States v. Karo*, 468 U.S. 705, 712 (1984). "It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence." *Id.*; *see also Knotts*, 460 U.S. at 284-85. Indeed, a major planned use of the Rule does not even involve the government reading the Remote ID message, but rather enables unmediated pilot-to-pilot signaling among private persons for coordinated, safe use of shared airspace.

Second, the brevity and occasional character of drone flights and the local nature of the Remote ID message makes the FAA's access to location information via Remote ID unlike the kind of "dragnet" electronic surveillance to which Brennan objects. Pet. Reply Br. at 13. "[R]elatively short-term monitoring of a person's movements" in public places "accords with expectations of privacy that our society has recognized as reasonable." *Jones*, 565 U.S. at 430 (Alito, J., concurring); *see also* 565 U.S. at 412 (citing *Knotts*, 460 U.S. at 281). The Rule requires drones to communicate Remote ID only from takeoff to shutdown. 86 Fed. Reg. at 4410-12. Based on a survey it conducted of more than 15,400 drone operators, the FAA notes

that private, recreational drone pilots conduct an average of only seven drone flights per month, totaling approximately 94 minutes of monthly flight time. FAA Br. at 29 (citing FAA, *FAA Aerospace Forecast: Fiscal Years 2020-2040* at 41-43, https://go.usa.gov/xMqTD). Unlike a cellphone, which has become "almost a 'feature of human anatomy'" that "tracks nearly exactly the movements of its owner," *Carpenter*, 138 S. Ct. at 2218, nothing in the record before us suggests that Remote ID location information provides any such "intimate window into a person's life," *id*. at 2217. Requiring a person during occasional short flights to identify in real time and share her drone system's momentary whereabouts on a local radio frequency says little about anything else in her life.

The limited, local, real-time information sharing the Rule requires is a far cry from the continuous surveillance the Supreme Court has held violates reasonable expectations of privacy. In *Carpenter*, for example, the government accessed 127 days' worth of defendants' cell phone location data providing "a detailed and comprehensive record of the person's movements," 138 S. Ct. at 2217, amounting to "near perfect surveillance" akin to what can be achieved by an ankle monitor, *id.* at 2218. And in *Jones*, the privacy invasion arose from the government surreptitiously attaching a GPS monitor to the defendant's car, 565 U.S. at 404 & n.2, and "catalogu[ing] every single movement" of the car for 28 days, 565 U.S. at 430 (Alito, J., concurring in the judgment); *accord id.* at 415 (Sotomayor, J., concurring). No physical trespass is asserted here, and, unlike cell-cite location data or a GPS tracker on a car, it is unclear how a drone system's Remote ID could be used to place anyone at the scene of a robbery or follow him to a drug stash house, *cf. Carpenter*, 138 S. Ct. at 2212-13*; Jones*, 565 U.S. at 402-04, nor how it could "reflect[] a wealth of detail" about a drone pilot's "familial, political, professional, religious, and sexual associations," 565 U.S. at

415 (Sotomayor, J., concurring). The drone system's real-time location data says nothing qualitative about the nature of the location nor the operator's relationship to it (e.g. whether he is at his home). Beyond the general concerns he raises about the intrusive capabilities of electronic surveillance, Brennan offers no specifics about how Remote ID anonymized messaging of a drone system's location during flight could reveal private facts or constitute governmental abuse in derogation of the Fourth Amendment.

We also see no basis to conclude that the FAA or other government actors will devote the time and resources Brennan assumes they will to exploit the Rule to somehow conduct extended surveillance. *See, e.g.*, *Jones*, 565 U.S. at 429 & n.10 (Alito, J. concurring in the judgment) (distinguishing ease of long-term surveillance with GPS from "exceptionally demanding" surveillance aided by limited-range radio transmitter that "could be lost if the police did not stay close enough"); *Obama v. Klayman*, 800 F.3d 559, 567 (D.C. Cir. 2015). As a practical matter, Remote ID messages are not readily available for collection from a centralized location but are detectible only within the ambit of a local radio signal—which Brennan calculates to be about a one-mile radius around the drone. 86 Fed. Reg. at 4428; *see also* Pet. Br. at 26; Pet. Reply Br. at 12. As a legal matter, despite Brennan's assumptions to the contrary, *see* Pet. Br. at 21, the Rule does not authorize aggregation and storage of flight data for later law-enforcement querying. The Final Rule abandoned the internet-based Remote ID proposal requiring private service providers to log Remote ID information from drone flights and store it for the FAA's later access, and the FAA has disavowed any plans under the Final Rule to log the data. U.S. DEP'T OF TRANSP., PRIVACY IMPACT STATEMENT at 10, J.A. 221.

Third, the Rule appropriately limits access to personally identifying information in the FAA's possession that could be linked to a drone's Remote ID message to reveal who owns the drone system. Remote ID does not reveal the pilot's or owner's identity, address, phone number, or other personal information. Rather, the message shows the drone's unique identification number; the latitude, longitude, and geometric altitude of the drone and of its controller; the drone's velocity; a time mark; and any applicable "emergency status" alert. 86 Fed. Reg. at 4410, 4412. That information itself is anonymized. The unique identifier—the drone's serial number—does not disclose who is flying the drone, whether it be the registered owner of the device or someone else.

The Rule authorizes the FAA alone to match the drone's nonpublic serial number to registration information, which includes the owner's name and contact information, and to use that personally identifying information only for airspace safety and security purposes relating to the drone's operation. The Rule's preamble specifies that "registration data pertaining to individuals is protected in accordance with the requirements of the Privacy Act (5 U.S.C. 552a)." 86 Fed. Reg. at 4433. Any use of Remote ID data, including by law enforcement personnel, "is bound by all Constitutional restrictions and any other applicable legal restrictions." *Id.* at 4435; *accord id.* at 4433.

Consistent with those limitations, the Remote ID Rule does not, without further regulatory action, authorize law enforcement personnel to access drone owners' personally identifying information separate from the FAA's involvement. The FAA emphasized that the Rule "does not speak to the use of information by law enforcement agencies or how remote identification data will be correlated with other law enforcement data." *Id.* at 4436. As the agency acknowledged,

amendment of its existing recordkeeping system for personally identifying information protected by the Privacy Act, *see* Department of Transportation System of Records Notice DOT/FAA-801, 81 Fed. Reg. 54,187 (Aug. 15, 2016), would be required before law enforcement could access registration information to match it with Remote ID data for uses beyond aviation safety and security, FAA Br. at 12-13, 31 n.4. And any new or updated System of Records must be published in the Federal Register for notice and public comment before implementation. *See* 5 U.S.C. § 552a(e)(4)(D), (e)(11). Nothing about the Rule itself supports Brennan's assertions that it will be used by government in ways that violate drone pilots' privacy rights. To be sure, it is possible that one day government or law enforcement collection of drone system operation data in and of itself could violate a pilot's constitutionally cognizable privacy interest. But Brennan has not shown that such data collection offends the Fourth Amendment in every application of the Rule to the typically very public activity of drone piloting.

Because we hold Brennan's Fourth Amendment facial challenge fails to establish that the Remote ID Rule requires drone operators to submit to warrantless intrusion on their constitutionally cognizable privacy interests, we need not and do not here address the government's alternative argument that an exception to the warrant requirement applies.

We likewise express no opinion on the potential viability of any as-applied Fourth Amendment challenge to specific applications of the Remote ID Rule. We thus do not foreclose the possibility of a declaratory judgment or injunctive action by a party establishing that application of the Remote ID Rule to its own specifically delineated drone uses would subject it to an unconstitutional privacy deprivation. *See generally Alvin Lou Media, Inc v. FCC*, 571 F.3d 1, 8 (D.C. Cir. 2009)

(challenge to rule's application permissible outside 30-day deadline to challenge the underlying rule); *Indep. Cmty. Bankers of Am. v. Bd. of Governors of Fed. Reserve Sys.*, 195 F.3d 28, 34-35 (D.C. Cir. 1999) (same). Nor do we pass on the viability of Fourth Amendment objections that might be raised on the specific facts of enforcement actions. But Brennan does not establish here that the putative privacy breaches he fears, such as continuous tracking of his every movement, or intrusion on the privacy of his home, are imminent or have yet occurred.

Because the Remote ID Rule itself "at most authorizes—but does not mandate or direct" the subcategory of applications that Brennan identifies as "searches" subject to the Fourth Amendment, his allegations are too conjectural to support standing to challenge such application. *Clapper v. Amnesty Int'l*, 568 U.S. 398, 412 (2013) (formatting modified). We may grant declaratory relief to a petitioner facing "a threat of injury which is sufficiently direct and immediate to constitute more than a string of contingencies or speculative characterizations," *Branch v. FCC*, 824 F.2d 37, 41 (D.C. Cir. 1987), but no such relief is available where key facts have not "crystallized" and it remains to be seen whether the government will ever use the challenged legal authority unlawfully, *City of Houston v. Dep't of Hous. and Urb. Dev.*, 24 F.3d 1421, 1431 (D.C. Cir. 1994). For the reasons already discussed, we do not read the Rule on its face to pose a direct and immediate threat of continuous law enforcement monitoring or intrusions on the privacy of the home.

Because Brennan has not established here that, in every application, the Remote ID Rule authorizes warrantless searches in violation of a reasonable expectation of privacy protected by the Fourth Amendment, we reject his constitutional claim.

II. Procedural claims

Brennan asserts the Remote ID Rule is arbitrary and capricious in various ways. 5 U.S.C. § 706(2)(A). None of those challenges succeeds.

A. No *ex parte* communication affected the Rule

Brennan argues that the FAA engaged in secret, *ex parte* communications that shaped the Final Rule but evaded public comment. He points to the FAA's convening of an industry group (the Cohort) in early 2020 to give the agency technical advice on its proposed network-based Remote ID system, its work with a NASA drone traffic management pilot program simultaneously with the development of the Remote ID Rule, and its demonstration of Remote ID capabilities to a group of public and private observers at the Federal Bureau of Investigation Academy. Brennan asserts that the FAA should now be required to publish a new or supplemental notice of proposed rulemaking to fully disclose the information he asserts the agency drew from those interactions.

Statutory requirements of public notice and comment ensure that rules are openly developed, subjected to effective comment from interested parties, and judicially reviewable on a materially complete record. "[T]he very legitimacy of general policymaking performed by unelected administrators depends in no small part upon the openness, accessibility, and amenability of these officials to the needs and ideas of the public from whom their ultimate authority derives, and upon whom their commands must fall." *Sierra Club v. Costle*, 657 F.2d 298, 400-01 (D.C. Cir. 1981). As relevant here, APA Section 4 obligates the FAA to publish notice of its proposed rulemakings, to "give interested persons an opportunity to participate in the rule making" by submitting comments, to

consider those comments, and then to "incorporate in the rules adopted a concise general statement of their basis and purpose." 5 U.S.C. § 553(c).

The APA contains no explicit bar on *ex parte* communications during a rulemaking process like this one, and communications that do not materially influence the action taken do not run afoul of APA requirements of notice-and-comment rulemaking. *See Vt. Yankee Nuclear Power Corp. v. Nat. Res. Def. Council*, 435 U.S. 519, 523-24 (1978); *Costle*, 657 F.2d at 402-03; *Home Box Off., Inc. v. FCC*, 567 F.2d 9, 57 (D.C. Cir. 1977). *Ex parte* communications may nonetheless violate the APA if "it appears from the administrative record under review that they may have materially influenced the action ultimately taken." *Action for Child.'s Television v. FCC*, 564 F.2d 458, 476 (D.C. Cir. 1977).

Brennan has not shown that the Remote ID Rule was materially affected by any *ex parte* influence, nor has he identified any harm he might have suffered if it were. *See id.* at 477. The Cohort the FAA convened was to advise on an approach to Remote ID that Brennan himself opposed in his comment and that the agency did not include in the Final Rule. The Proposed Rule would have relied primarily on the internet to communicate Remote ID, with private companies under contract with the FAA acting as Unmanned Aircraft System Service Suppliers monitoring drone flights via the internet and collecting and storing that internet-transmitted flight data for the FAA's access. Proposed Rule, 84 Fed. Reg. at 72,439, 72,467-68, 72,499. "Under this concept, the aircraft's control station (often a mobile phone) would connect to the internet and transmit remote identification information to a third-party service provider." Final Rule, 86 Fed. Reg. at 4405. During the comment period for the Proposed Rule, the FAA convened a Cohort of private companies with experience in remote

identification of drone locations to help the agency develop technical parameters it envisioned would be contractually required of the Service Suppliers. *See id*. at 4406; *see also* Proposed Rule, 84 Fed. Reg at 72,484-85. But because it ultimately concluded that a system of real-time remote identification relying on local radio bandwidth "will be adequate," *id.* at 4408, the FAA dropped the proposed requirement that drones use internet for Remote ID and that the FAA access their information as collected by Service Suppliers.

Brennan objects that FAA staff met with the Cohort but did not include the details of those meetings in the public record, making it impossible for the public to comment on them. But the FAA received and responded to thousands of comments on the internet-based proposal. More to the point, Brennan has not shown that information the FAA obtained from the Cohort meetings had any material bearing on the Final Rule. The FAA's decision to table reliance on internet-based transmission in favor of the simpler, cheaper, and more secure radio-broadcast system rendered irrelevant the technical capabilities the Cohort had been asked to consider, and the Rule's preamble elaborates on the many reasons supporting that decision. Final Rule, 86 Fed. Reg. at 4405-09, 4491-92.

The FAA noted that "[t]he primary challenge with [the internet-based] concept is its reliance on Wi-Fi or cellular network service being available where an aircraft is flying; the concept would not work in areas lacking cellular telephone coverage." *Id*. at 4405. Relatedly, the FAA concluded the Final Rule's reliance on a radio-broadcast system avoids unnecessary costs to drone users of equipment and Wi-Fi data plans associated with the internet-based proposal. *Id*. at 4406-07, 4409. And, even where reliable internet is available and drone pilots subscribe to it, the agency noted commenters'

observation that "cellular networks are optimized to work with ground-based equipment rather than airborne equipment," so they might not readily support Remote ID of drones in flight. *Id*. at 4407.

Security was also a major concern with the internet-based proposal. Based on comments explaining that tracking drone flights via the internet would leave them vulnerable to cyberattacks, deliberate interference, and security and data breaches by individuals, non-State actors, and foreign governments, the FAA was persuaded that reliance on radio frequency would, at least initially, best serve the Remote ID Rule's objectives. *Id*. at 4406-07, 4409. The FAA concluded that "a broadcast-only solution is sufficient, for the time being and given the types of unmanned aircraft operations that are currently allowed, to maintain the safety and security of the airspace of the United States" in line with authorized operations and airspace regulations. *Id*. at 4409.

Even if the Final Rule had not rendered the Cohort superfluous, the FAA's ground rules for Cohort meetings put discussion of the Proposed Rule off limits; the agency directed members who wished to comment to do so via the public rulemaking docket. *See* FAA Br. at 40-41. Brennan nonetheless contends that the Cohort must have affected the Final Rule because the preamble mentions the Cohort's identification of unforeseen issues with "significant technical and regulatory requirements that go beyond existing industry consensus standards," and notes "the challenge of developing and issuing technical specifications to govern remote identification interoperability when producers of [unmanned aircraft systems] have not yet designed" drones with Remote ID capability. Final Rule, 86 Fed. Reg. at 4406. But those reported difficulties are symptomatic of more fundamental problems that the Rule fully documents without reference to

the Cohort as such—even as it cites Cohort members' duly submitted public comments. *Id.* at 4408 (citing comments of Amazon Prime Air, Verizon, Skyward, and AirMap).

In sum, the FAA's Final Rule relied on extensive evidence independent of whatever it might have learned from the Cohort, and Brennan has failed to show that the agency's communications with the Cohort outside the rulemaking process had any effect on the Rule.

The two other interactions that Brennan contends amounted to impermissible *ex parte* influences on the Final Rule are even further from the mark. One was the FAA's work with NASA on drone traffic control, which is an important but distinct component of the agency's efforts to integrate safe and efficient drone flight into the national airspace. The Remote ID Rule did not discuss or depend on the FAA's collaboration with NASA regarding drone traffic management. Rather, when Congress in the 2016 FAA Extension Act directed the FAA to develop requirements for remote identification of drones and drone pilots during flight, now reflected in the Remote ID Rule, it also asked the FAA to continue ongoing research collaboration with NASA on unmanned aircraft system traffic management. Pub. L. No. 114-190, § 2208, 130 Stat. at 633-34. The first phase of the traffic management study concluded in October 2019, after the Proposed Rule's comment period closed; the second, pursuant to the 2018 FAA Reauthorization Act, Pub. L. No. 115-254, § 376(b), 132 Stat. at 3314-15, tested traffic management systems with drones remotely identified under the Final Rule after its publication. *See* FAA, *Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Pilot Program (UPP): UPP Summary Report* (Oct. 2019), https://go.usa.gov/xFmVU; FAA, *Unmanned Aircraft Systems (UAS) Traffic Management (UTM) UTM Pilot Program (UPP) Phase Two (2) Progress Report* (Mar. 2021),

https://go.usa.gov/xFmy9; FAA, *Uncrewed Aircraft Systems (UAS) Traffic Management (UTM) UTM Pilot Program (UPP) Phase 2 Final Report* (July 2021), https://go.usa.gov/xFmyU. The Remote ID Rule plainly was not influenced by the asserted *ex parte* input from NASA.

Finally, Brennan sees illegitimate *ex parte* influence in a demonstration the FAA conducted at the FBI Academy in Quantico to show "detect and display information about unmanned aircraft operation below 400 feet." FAA Memorandum, Summary of the Technology Demonstration Regarding *Remote Identification of Unmanned Aircraft Systems* Notice of Proposed Rulemaking, Docket No. FAA-2019-1100 (Sept. 30, 2020). Pointing to a four-page FAA memo that describes the demonstration, which included a question-and-answer session Brennan learned of through a FOIA request, *id*.; *see also* Pet. Br. at 12 n.8, Brennan asserts that the public was improperly denied notice and an opportunity to comment on "the details of the Remote ID demonstration for law enforcement officials, and the complete explanation of how this data will be used and stored for law enforcement purposes," Pet. Br. at 37. Brennan does not identify how he believes the demonstration or related discussion, neither of which are mentioned in the Final Rule, could have affected it, but his references to data use and storage by law enforcement appear to relate to his Fourth Amendment concerns. As already discussed, the Final Rule does not authorize data storage nor use by non-aviation law enforcement, and Brennan's concerns about such eventualities are misplaced or premature.

In sum, none of the communications Brennan identifies as "*ex parte*" affected the integrity of the notice and comment process and thus the validity under the APA of the Remote ID Rule.

B. The Final Rule was a logical outgrowth of the Proposed Rule

Brennan asserts that two requirements of the Final Rule "do not logically stem from the notice provided in the [Proposed Rule], rendering those aspects of the rule void." Pet. Br. at 39. He objects to the change from measuring the reported altitude of drone control stations using barometric pressure altitude to measuring it geometrically with GPS, and to the elimination of the internet-based "Limited Remote Identification" option for retrofitting existing drones in favor of the radio-broadcast module option.

To comport with the APA's notice-and-comment requirements, an agency's final rule must be a logical outgrowth of the version set forth in its notice of proposed rulemaking. *Covad Comms. Co. v. FCC*, 450 F.3d 528, 548 (D.C. Cir. 2006). If it were otherwise, agencies could evade their notice-and-comment obligations by adopting final rules unrelated to their published proposals. An agency may not leave the public to "divine [the agency's] unspoken thoughts" on a final rule "surprisingly distant from the proposed rule." *CSX Transp., Inc. v. Surface Transp. Bd.*, 584 F.3d 1076, 1080 (D.C. Cir. 2009) (citing *Int'l Union, United Mine Workers of Am. v. Mine Safety & Health Admin.*, 407 F.3d 1250, 1259-60 (D.C. Cir. 2005) (formatting modified)). At the same time, the APA does not require that rules be subjected to multiple cycles of notice and comment until the version adopted as final is identical to the last notice of proposed rulemaking; after all, the very premise of agencies' duty to solicit, consider, and respond appropriately to comments is that rules evolve from conception to completion. The public right to have a say in such development is honored so long as affected parties "should have anticipated" the final rule in light of the notice. *Covad Comms. Co.*, 450 F.3d at 548. Notice suffices when it has

"expressly asked for comments on a particular issue or otherwise made clear that the agency was contemplating a particular change." *CSX Transp.*, 584 F.3d at 1081.

The change from barometric pressure to geometric altitude in the Remote ID Rule was no surprise. The FAA proposed to include the altitude of a drone's control station as a Remote ID message element to enable the agency to "locate an operator in circumstances under which the person manipulating the flight controls . . . is not at ground level, such as a person operating a [drone] from the roof of a building." Final Rule, 86 Fed. Reg. at 4420. The Proposed Rule acknowledged that only one form of altitude measurement was needed, and it favored using barometric pressure. Proposed Rule, 84 Fed. Reg. at 72,473. The FAA initially reasoned that barometric pressure is more precise and is the standard way altitude is measured in aviation. Final Rule, 86 Fed. Reg. at 4420. Nonetheless, the agency requested comment on whether both barometric pressure and geometric altitude measurements should be part of the Remote ID message. Proposed Rule, 84 Fed. Reg. at 72,473.

After reviewing comments favoring geometric altitude's compatibility with existing drone technologies, the FAA elected in the Final Rule to require only geometric altitude measurement. "Many commenters recommended using geometric altitude for control stations, suggesting that it would be of greater usefulness, reliability, and less technically complex to integrate into" unmanned aircraft systems. Final Rule, 86 Fed. Reg. at 4420. Whereas drone control stations are not ordinarily equipped with the barometric pressure sensors used on airplanes, making compliance with that requirement "difficult and costly," most existing smart devices typically used as control stations for recreational drones are equipped with GPS that measures geometric altitude. *Id.* Barometric pressure instruments also require more calibration, testing, and

maintenance than GPS. *Id*. The Final Rule thus requires the Remote ID signal to include the location of the drone and its control-station or takeoff location using geometric instead of barometric pressure altitude. *See id.* at 4422-23 (concerning the drone's altitude), 4431-32 (concerning the altitude of a Broadcast Module drone's takeoff location).

Brennan objects that the "FAA requested comment on whether both geometric and barometric should be transmitted," thus giving "no indication" that GPS alone might be used, or of the degree of accuracy the FAA would require of GPS altitude measurements. Pet. Br. at 41 (formatting modified). But it remains a mystery how requiring one altitude measurement rather than both could be prejudicial. As for the accuracy the FAA requires of GPS, the agency explained that it was "adopting a geometric altitude accuracy requirement that is compatible with the performance requirements being established for cellular service providers under the E911 mandate that allows emergency service providers to accurately locate the geographic position of the mobile device." Final Rule, 86 Fed. Reg. at 4431. In view of the FAA's call for comments on both barometric and geometric altitude, Brennan had the requisite opportunity to comment on the achievable accuracy of GPS—an opportunity taken up by other commenters. *See, e.g.*, Walter Bender, Remote ID NPRM Comments at 1 (Mar. 3, 2020), https://www.regulations.gov/comment/FAA-2019-1100-50995 (analyzing and recommending accuracy requirements for both barometric and GPS altitude measurements); Gregory Walden, Comments of the Small UAV Coalition at 24-25 (Mar. 2, 2020), https://www.regulations.gov/comment/FAA-2019-1100-50278 (same). At bottom, Brennan's objection to including accurate GPS location-identification information in Remote ID messaging appears to be a variant of his Fourth

Amendment privacy claim and fails for the reasons explained above.

Brennan's contention that the Proposed Rule gave no notice of the radio broadcast module option in the Final Rule also fails. Under the Rule, owners of drones incapable of broadcasting the requisite Remote ID message who wish to fly their drones outdoors outside of an FAA-recognized identification area may do so by retrofitting their drones with broadcast modules to meet the Rule's Remote ID requirements. Brennan insists that he lacked the chance to voice concerns that a broadcast module would cause radio frequency interference problems with certain types of equipment that would negatively affect its use. But the FAA invited comment on the viability of a broadcast module option. Proposed Rule, 84 Fed. Reg. at 72,490. The call for comments stated that any retrofit module would have to comply with Remote ID requirements, which in the Proposed Rule included use of radio broadcasts or internet transmissions. Members of the public had the opportunity to voice their concerns that retrofitting certain drones with radio broadcast modules could interfere with radio signals used for navigation, video recording, or any other specialized function.

Because the Final Rule was a logical outgrowth of the Proposed Rule, Brennan had notice of and the opportunity to comment on the features to which he now objects.

C. There was no consultation failure

Brennan contends that, despite Congress's express directive that it do so, the FAA somehow fell short of fulfilling its statutory duty to consult on the Remote ID standards with the President of the Radio Technical Commission for Aeronautics, Inc. (RTCA) and the Director of the National

Institute of Standards and Technology (NIST). FAA Extension Act § 2202(a), 130 Stat. at 629. His complaint seems to be that the "FAA's ID Area requirement is not based on any standards developed by or in coordination with the [stakeholder] group as mandated by Congress." Pet. Br. at 46. Brennan claims that the FAA thereby failed to fulfill what he sees as "a statutory prerequisite to its rulemaking authority" that requires us to vacate the Rule. Pet. Reply Br. at 31.

The FAA involved the RTCA and NIST in its preparation for and development of the Rule, just as Congress directed. The RTCA is a nonprofit organization that provides technical guidance on a range of aviation-related topics. *See* RTCA, *About us*, https://www.rtca.org/about. NIST is an agency within the Department of Commerce responsible for advancing measurement science, standards, and technology in coordination with government and industry. *See* NIST, *About NIST*, https://www.nist.gov/about-nist. The 2016 enactment Brennan invokes directed that:

> The Administrator of the Federal Aviation Administration, in consultation with the Secretary of Transportation, the President of RTCA, Inc., and the Director of the National Institute of Standards and Technology, shall convene industry stakeholders to facilitate the development of consensus standards for remotely identifying operators and owners of unmanned aircraft systems and associated unmanned aircraft.

FAA Extension Act § 2202(a), 130 Stat. at 629. That stakeholder convening was to consider remote identification requirements, including appropriate requirements for "different classifications of unmanned aircraft systems operations, including public and civil," and the feasibility of a

publicly available database "of unmanned aircraft and the operators thereof." FAA Extension Act § 2202(b), 130 Stat. at 629. The FAA was to report to Congress within the year on any standards developed, *id*. § 2202(c), 130 Stat. at 629, and to proceed within the following year to promulgate regulations or guidance implementing them, *id*. § 2202(d), 130 Stat. at 629.

The FAA duly consulted with the named entities, convened its Unmanned Aircraft Systems Identification and Tracking Aviation Rulemaking Committee comprised of interested stakeholders, and issued a report to Congress reflecting the requested recommendations. *See* FAA, ARC RECOMMENDATIONS FINAL REPORT (2017), J.A. 561-773. The RTCA served on the Committee, and NIST served as a government observer to the Committee. *See id.* Appendix A at 2, J.A. 617; FAA Br. at 63 (citing Letter from the FAA to Senator Roger Wicker, Chairman of U.S. Senate Committee on Commerce, Science, and Transportation 1 (Feb. 13, 2019), https://www.faa.gov/sites/faa.gov/files/2021-11/Letter-Report-re-Sec.-2202-of-P.L.-114-190-2.13.19-Provided-to-Congress_0.pdf); Pet. Reply Br. at 30 (acknowledging FAA-Wicker letter).

Brennan complains that the Aviation Rulemaking Committee "never considered or even mentioned the concept of an ID Area" as an option for Remote ID compliance. Pet. Br. at 46. But Congress did not require that the RTCA or NIST weigh in on every facet of the proposed rule. *See* FAA Extension Act § 2202(b), 130 Stat. at 629. Under the Final Rule, a person may operate an unmanned aircraft lacking remote identification capability only "at specific FAA-recognized identification areas." 86 Fed. Reg. at 4391. Brennan would prefer homeowners and local parks to be able to apply for ID Area status. *See* Pet. Br. at 58. But the FAA received and considered many comments on that issue. *See* 86

Fed. Reg. at 4414-17, 4437-38. The agency's determination in the Final Rule to limit eligibility to apply for ID-Area status to community-based organizations and educational institutions is not rendered invalid for want of evidence that the FAA consulted the RTCA or NIST on that point.

D. The FAA adequately responded to significant comments

Finally, Brennan accuses the agency of failing to heed "significant critical comments" that, had they been addressed, he says would "require a change in the rule." Pet. Br. at 46. He finds lacking the FAA's explanation of the Rule's legal grounding and constitutional limits, its calculation of the Rule's regulatory costs, and its treatment of drone hobbyists' interests.

The APA calls on us to determine whether an agency has considered and responded adequately to major substantive comments and, where it has failed to do so, remand for further proceedings. 5 U.S.C. § 706(2)(A); *see Sierra Club v. EPA*, 863 F.3d 834, 838 (D.C. Cir. 2017) (citing *Pub. Citizen, Inc. v. FAA*, 988 F.2d 186, 197 (D.C. Cir. 1993)). Our enforcement of this and other APA procedural duties helps to ensure fair treatment of people affected by agencies' rules. "To this end there must be an exchange of views, information, and criticism between interested persons and the agency" in which all significant factors are considered. *Home Box Office, Inc.*, 567 F.2d at 35. But exhaustiveness itself is not the measure. The agency must make clear the major policy issues at stake and why it resolved them as it did. It need not respond to every fact, idea, or opinion raised in comments, nor need it address speculative or plainly baseless concerns. *See id.* at 35-36 & n.58.

Brennan argues that the FAA failed to address various comments critical of the Proposed Rule. He says it overlooked comments that the Rule exceeds the agency's statutory authority to regulate drone operations only within the "navigable airspace" subject to FAA regulation, 49 U.S.C. § 40103(b), by instead purporting to apply throughout the "airspace of the United States," *id.* § 40103(a)(1), which he views as more encompassing. He also says that the Rule exceeds the scope of Congress's power to legislate pursuant to the Commerce Clause insofar as it applies to "the hobby of model aviation." Pet. Br. at 50. He asserts the FAA ignored comments that its criteria for ID Areas run afoul of due process (by restricting hobbyists' access to public airspace) and the First Amendment (by requiring as a condition of access to an ID Area association with the organization sponsoring it). And he accuses the FAA of sidestepping comments that the Rule authorizes warrantless intrusions on homeowners' privacy in violation of the Fourth Amendment.

In both the Proposed Rule, 84 Fed. Reg. at 72,451, and Final Rule, 86 Fed. Reg. at 4395, the FAA identified its statutory authority. *See* 49 U.S.C. §§ 40103(b)(2), 44805. The asserted constitutional concerns under the Commerce Clause, the Due Process Clause, and the First Amendment are either frivolous, or, like the Fourth Amendment concern, address potential future applications rather than the facial validity of the Rule itself, or both. The agency had no obligation to respond to comments "incapable of affecting the final rule." *City of Portland v. EPA*, 507 F.3d 706, 715 (D.C. Cir. 2007). And the FAA responded to Brennan's Fourth Amendment concerns. *See* 86 Fed. Reg. at 4435-36.

As for the FAA's treatment of regulatory costs, Brennan asserts the agency's cost calculations were artificially low because it failed to account for comments offering (1) higher

estimates of the time and labor required to apply for FAA-recognized ID Area designation and (2) higher aggregate drone retrofit cost estimates by assuming slower replacement with new Rule-compliant models. But the agency did address those cost issues. *See* Final Rule, 86 Fed. Reg. at 4481, 4483; *see also* FAA, REMOTE IDENTIFICATION OF UNMANNED AIRCRAFT SYSTEMS NOTICE OF PROPOSED RULEMAKING – PRELIMINARY REGULATORY IMPACT ANALYSIS 106-07 (Dec. 20, 2019), J.A. 337-38; FAA, REMOTE IDENTIFICATION OF UNMANNED AIRCRAFT FINAL RULE – REGULATORY IMPACT ANALYSIS 114-15 (Sept. 2020), J.A. 540-41. In any event, given that the FAA's total cost estimates range from $214 to $246 million, Final Rule, 86 Fed. Reg. at 4489, the differences in the FAA's and Brennan's estimates are slight; the adequacy of the FAA's response regarding what Brennan calculates as approximately $1.4 million more in certain indirect compliance costs that he asserts it should have considered is immaterial to the validity of the Rule.

Finally, Brennan faults the FAA's response to suggested accommodations of drone hobbyists seeking more places to fly and more freedom from the Rule's requirements. He asserts that the FAA "flat out did not respond" to the Academy of Model Aeronautics' comment that model aircraft should be excepted from the Rule. Pet. Br. at 57. But the FAA did acknowledge that suggestion; it excepted home-built drones made for educational or recreational purposes from design and production requirements, but not operational requirements. *See* Final Rule, 86 Fed. Reg. at 4449.

The FAA also gave a reasoned response to comments suggesting that homeowners and local governments be eligible to establish ID Areas in backyards and local parks. The FAA explained that it "intends most [unmanned aircraft systems] to identify remotely," and that operation without Remote ID at ID

Areas "is primarily for those who are truly unable to use either standard remote identification [drones] or remote identification broadcast modules." *Id*. at 4437. It defended the more limited expansion allowing educational institutions and community-based organizations to apply for ID Areas as "sufficient to meet the needs of student model flyers" while avoiding further expansion it feared could expand so far as to "undermine the effectiveness of remote identification." *Id*.

Brennan contends that the FAA did not adequately respond to comments questioning the safety rationale for the Rule—comments arguing that recreational drones have thus far caused few documented harms, and that Remote ID requirements have created rather than resolved safety risks to drone pilots. The Rule reasonably describes the benefits of Remote ID to mitigate a wide range of identified safety and security concerns. *See, e.g*, Final Rule, 86 Fed. Reg. at 4391, 4394-97, 4418-20, 4490; *see also* Proposed Rule, 84 Fed. Reg. at 72,454-55. Brennan acknowledges the agency's response to comments objecting that identification of drone pilots' location during flight can facilitate assaults against them and theft of their equipment; his dissatisfaction with the substance of the response relying on operator precautions and existing law and law enforcement to address such attacks is no reason to invalidate the Rule.

CONCLUSION

For all these reasons, we deny the petition for review.

So ordered.