CASE COMMENT:

BRENNAN V. DICKSON, 45 F.4TH 48 (D.C. CIR. 2022)

JOSEPH J. VACEK, J.D.*

ABSTRACT

The case *Brennan v. Dickson*¹ analyzes whether the Federal Aviation Administration's ("FAA") Remote Identification of Unmanned Aircraft rule (hereinafter "Remote ID" or "Rule") that requires small drones to broadcast a "digital license plate" constitutes a violation of privacy under the Fourth Amendment of the United States Constitution.² The court found that the Rule did not go beyond the limits of the Fourth Amendment, and that both Petitioner's facial challenge and procedural challenges to the Rule lacked merit, while preserving the ability of a future plaintiff's as-applied challenge. Despite acknowledging statutory and precedential differences between public, navigable airspace, and private airspace super adjacent to the surface estate, the court did not analyze the issue. The question to what extent the FAA has regulatory authority over private, non-navigable airspace remains unresolved.

^{*†} Joseph Vacek is an Associate Professor in the School of Aerospace Sciences at the University of North Dakota. He teaches aviation law, drone law, and other courses.

^{1. 45} F.4th 48 (D.C. Cir. 2022).

^{2.} Remote Identification of Unmanned Aircraft, 86 Fed. Reg. 4390, 4396 (Jan. 15, 2021) (to be codified at 14 C.F.R. pts. 1, 11, 47, 48, 89, 91, 107) [hereinafter *Final Rule*].

I. FACTS
II. LEGAL BACKGROUND235
A. PETITIONERS CLAIMS THE REMOTE ID RULE ALLOWS UNREASONABLE LOCATION TRACKING236
B. PETITIONER CLAIMS REMOTE ID RULE DISREGARDS PRIVATE PROPERTY237
III. ANALYSIS
A. THE COURT REJECTED PETITIONER'S FACIAL CHALLENGE TO THE REMOTE ID RULE238
B. REMOTE ID BROADCAST DOES NOT RUN AFOUL OF THE FOURTH AMENDMENT239
1. The Remote ID Rule calls for installation, not monitoring by law enforcement240
2. The characteristics of drone operations make governmental "dragnet" surveillance unlikely240
3. The Remote ID rule limits access to personally identifying information241
C. Drone Operators Lack Any Reasonable Expectation of Privacy of Their Drone Systems During Flight241
IV. IMPACT
A. ALL DRONE OPERATORS MUST COMPLY WITH THE REMOTE ID RULE, EVEN THOSE FLYING IN PRIVATE AIRSPACE243
B. THE COURT DID NOT DISTINGUISH PUBLIC VERSUS PRIVATE AIRSPACE
V. CONCLUSION244

I. FACTS

Approximately three years ago, the FAA published a notice of proposed rulemaking for Remote ID, proposing a rule for small drones that would require small drone operators to broadcast certain identifying elements continuously during flight.³ The final rule was published on January 15,

^{3.} Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438, 72439 (proposed Dec. 31, 2019) (to be codified at 14 C.F.R. pts 1, 47, 48, 89, 91, 107).

2021, with an effective date of March 16, 2021.4 On March 10, 2021, the effective date was extended to April 21, 2021.5 On March 12, 2021, Petitioners filed suit in the D.C. Circuit challenging the Rule on its face.6 The D.C. Circuit published its opinion on July 29, 2022, upholding the Rule.7 The FAA has again extended the compliance deadline, this time to September 16, 2023.8

The Remote ID rule requires small drone operators to continuously broadcast a "digital license plate" consisting of five identifying elements: (1) a unique identification number, (2) its position described by latitude, longitude, altitude, and velocity, (3) the operator's position, (4) a time stamp, and (5) abnormal drone status, if applicable—e.g., engine failure or the like.⁹ The broadcast information and the equipment used to broadcast it must meet minimum compliance requirements, namely: that the drone's operation must be dependent upon a successful self-test, such that it is rendered incapable of flight if the Remote ID equipment is not functioning;¹⁰ the Remote ID equipment must not be able to be disabled by the operator;¹¹ the Remote ID data must be broadcast over the unlicensed radio frequency spectrum band (wifi);¹² and the Remote ID broadcast equipment must be designed to maximize the range at which the broadcast can be received.¹³

The only method for small drones unequipped with Remote ID equipment to be operated is either indoors or within FAA Recognized Identification Areas, 14 which are for small drone enthusiast clubs. 15

II. LEGAL BACKGROUND

The Remote ID rule came about in the context of tension between Congressional directives for the FAA to both encourage the development and use of drones¹⁶ and to create a regulatory framework to protect the safety and

^{4.} Final Rule, supra note 2 at 4390.

^{5.} Remote Identification of Unmanned Aircraft; Delay, 86 Fed. Reg. 13629 (Mar. 10, 2021) (to be codified at 14 C.F.R. pts. 1, 11, 47, 48, 89, 91, 107).

^{6.} Brief of Petitioners at 1, Brennan v. Dickson, 45 F.4th 48 (D.C. Cir. 2022) (No. 21-1087).

^{7.} Brennan, 45 F.4th at 73.

^{8.} Remote Identification for Drone Pilots, FAA, https://www.faa.gov/uas/getting_started/remote_id/drone_pilots#:~:text=All%20drone%20pilots %20required%20to,time%20to%20upgrade%20their%20aircraft (last visited Oct. 20, 2022).

^{9.} Final Rule, supra note 2, at 4391.

^{10.} Id. at 4414.

^{11.} Id. at 4410.

^{12.} Id. at 4495.

^{13.} Id. at 4427.

^{14.} See id.; FAA-Recognized Identification Areas (FRIAs), FAA, https://www.faa.gov/uas/getting_started/remote_id/fria (last visited Oct. 24, 2022).

^{15.} FAA-Recognized Identification Areas (FRIAs), supra note 14.

^{16.} FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, §§ 332, 333 126 Stat. 11, 73-76.

security of U.S. airspace and its users from drones.¹⁷ The FAA Reauthorization Act of 2016 directed the FAA to develop a method of locating small drones and their operators.¹⁸ Five years later, the FAA published the Remote ID rule in 2021.¹⁹ The Remote ID rule's stated purpose is to "provide airspace awareness to the FAA, national security agencies, law enforcement entities, and other government officials"²⁰ and to deter unsafe flying by drone operators,²¹ with the benefits of the Rule as "enabl[ing] better threat discrimination, an immediate and appropriate law enforcement response, and a more effective follow-on investigation."²² The burden on drone operators complying with the Remote ID rule includes a requirement to broadcast the Remote ID signal while the drone is airborne,²³ which requires the installation of special broadcast equipment on the drone either by the manufacturer or by retrofit.²⁴

A. PETITIONERS CLAIMS THE REMOTE ID RULE ALLOWS UNREASONABLE LOCATION TRACKING

Petitioner Brennan claimed the Remote ID rule requiring small drones to continuously broadcast certain identifying information during flight amounted to unreasonable location tracking.²⁵ He also raised procedural issues related to various claimed insufficiencies in the rulemaking process required by the Administrative Procedure Act.²⁶ Most of the procedural claims will be ignored for the purposes of this Comment. Brennan's petition was a facial challenge, as he did not assert any injury that would otherwise grant standing.²⁷

In his challenge, Brennan argued the Remote ID rule's requirement would allow continuous GPS tracking of small drones, which amounted to an overreach "into private property and reasonable expectations of privacy [and] cannot survive Constitutional review." He supports his substantive overreach claim by arguing the Rule is an unconstitutional search of the

^{17.} FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 349, 132 Stat. 3186, 3299 (codified at 49 U.S.C. § 44809(f)).

^{18.} FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 2202(a), 130 Stat. 615, 629.

^{19.} Final Rule, supra note 2, at 4390.

^{20.} Id. at 4393.

^{21.} Id. at 4490.

^{22.} *Id.* at 4435.

^{23.} See id. at 4390.

^{24.} See id. at 4428.

^{25.} Brief of Petitioners, supra note 6, at 6.

^{26.} Id. at 30-64.

^{27.} Id. at 4.

^{28.} Id. at 20.

curtilage,²⁹ that it infringes upon the privacy interests of small drone operators and the people in general,³⁰ that it allows an unlimited time length of tracking,³¹ and that it allows more intrusive tracking than is constitutionally allowed.³² Brennan articulated a substantive argument of constitutional and statutory overreach by the FAA in regulating low altitude airspace in violation of United States Supreme Court precedent, but framed it as a procedural matter.³³ The court dismissed it as insignificant in its opinion.³⁴

B. PETITIONER CLAIMS REMOTE ID RULE DISREGARDS PRIVATE PROPERTY

The reach of the broadcast requirement is claimed by Petitioner to go too far in *Brennan*. The Remote ID rule requires that he continuously broadcast five identifying elements.³⁵ Brennan's core substantive argument contended the sum of the information required to be broadcast by the Remote ID rule amounts to unreasonable location tracking and infringed on his reasonable expectations of privacy as a warrantless search.³⁶ Brennan structured his reasonableness argument on the differentiation between navigable and nonnavigable airspace,³⁷ arguing that the requirement of continuous broadcast goes too far because it requires individuals to broadcast in their curtilage³⁸ and private airspace.³⁹ He claimed the FAA ignored the distinction between navigable and non-navigable airspace in requiring continuous broadcast, and that "[t]he final rule's use of the term 'airspace of the United States' claims unfettered authority to regulate all airspace, including down to non-navigable airspace in a private backyard."⁴⁰

Brennan claimed the identification information required to be broadcast goes beyond the limits of location identification and information specificity found to be acceptable by the Supreme Court in *United States v. Jones*⁴¹ or

^{29.} Id. at 22.

^{30.} Id. at 24.

^{31.} Id. at 27.

^{32.} Id.

^{33.} Id. at 49-50 (citing to United States v. Lopez, 514 U.S. 549 (1995)).

^{34.} Brennan, 45 F.4th at 72.

^{35.} See supra note 12 and accompanying text.

^{36.} Brief of Petitioners, supra note 6, at 20-21.

^{37.} Id. at 50-52.

^{38.} Id. at 22.

^{39.} Id. at 24.

^{40.} Id. at 52.

^{41. 565} U.S. 400, 404 (2012) (holding the government's four-week long GPS monitoring of a vehicle as an unconstitutional search).

Carpenter v. United States⁴² Brennan argued Jones and Carpenter are applicable and that Remote ID allows "tracking with a pinpoint in terms of feet"⁴³ where the technology used in Jones and Carpenter was found to be less precise⁴⁴ yet still violated the Fourth Amendment.⁴⁵ Brennan argued, therefore, that Remote ID results in impermissibly intrusive tracking.⁴⁶

III. ANALYSIS

Judge Pillard of the D.C. Circuit drafted the opinion, after oral arguments before Judges Pillard, Wilkins, and Walker.⁴⁷ The court held Brennan's facial challenge was insufficient to support vacatur of the Rule, and Brennan did not show any actual harm or imminent threat of harm; therefore, there was also no justiciable as-applied challenge.⁴⁸ However, the court preserved the possibility of a future as-applied challenge to the Remote ID rule.⁴⁹

A. THE COURT REJECTED PETITIONER'S FACIAL CHALLENGE TO THE REMOTE ID RULE

Brennan argued the Rule allows government overreach and therefore violates the Fourth Amendment on its face.⁵⁰ A facial challenge to a Rule contends that the Rule is unconstitutional as written.⁵¹ Though a disfavored vehicle, the court entertained the facial challenge.⁵² For a facial challenge to succeed, a plaintiff "must establish that no set of circumstances exists under which the [rule] would be valid."⁵³ While Brennan raised several instances showing how a drone operator required to broadcast Remote ID data might attempt to state a claim based upon the operators location within a home or its curtilage,⁵⁴ the court reasoned that "[i]dentifying potential applications of the rule that could be unlawful is not enough[,]"⁵⁵ and the court was not

^{42. 138} S. Ct. 2206, 2219 (2018) (holding the government violated the petitioner's reasonable expectation of privacy by accessing his cell phone location information for investigative purposes).

^{43.} Brief of Petitioners, supra note 6, at 29.

^{44.} Id. at 28-29.

^{45.} Id.; see Jones, 565 U.S. at 404; Carpenter, 138 S.Ct. at 2219.

^{46.} Brief of Petitioners, supra note 6, at 29-30.

^{47.} Brennan v. Dickson, 45 F.4th 48, 53 (D.C. Cir. 2022).

^{48.} Id. at 54.

^{49.} Id. at 65.

^{50.} Brief of Petitioners, supra note 6, at 49.

^{51.} See Brennan, 45 F.4th at 61.

^{52.} *Id.*; Wash. State Grange v. Wash. State Republican Party, 552 U.S. 442 (2008) ("Claims of facial invalidity often rest on speculation. As a consequence, they raise the risk of 'premature interpretation of statutes on the basis of factually barebones records.") (quoting Sabri v. United States, 541 U.S. 600, 609 (2004)).

^{53.} Brennan, 45 F.4th at 61 (alteration in original) (quoting Ass'n of Priv. Sector Colls. & Univs. v. Duncan, 681 F.3d 427, 442 (D.C. Cir. 2012)).

^{54.} Id. at 62; Brief of Petitioners, supra note 6, at 23.

^{55.} Brennan, 45 F.4th at 61 (citing Sherley v. Sebelius, 644 F.3d 388, 397 (D.C. Cir. 2011)).

required to "'resolve every hypothetical presented' by Brennan."⁵⁶ Thus, the court quickly rejected the facial challenge, reasoning that the Remote ID rule did not exceed the FAA's statutory authority under the APA and, therefore, was facially valid.⁵⁷ Nonetheless, the court addressed Brennan's Fourth Amendment challenges; the court reasoned that "drones are virtually always flown in public[; therefore,] [r]equiring 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."⁵⁸ The use of "open air" by the court is a direct analogy to the "open fields" exception of the Fourth Amendment, indicating the court acknowledged the potential for future law enforcement abuse of the Remote ID technology, and explicitly held open the possibility of an asapplied challenge.⁵⁹

B. REMOTE ID BROADCAST DOES NOT RUN AFOUL OF THE FOURTH AMENDMENT

To the substance of the technical argument Brennan raised, the court found that none of the five discrete information "packets," individually or together, required to be broadcast by the Remote ID rule, are protected as private under Fourth Amendment precedent, noting "[i]t is hard to see what could be private about flying a drone in the open air." for the court stated that "[d]rones fly in the open, and people ordinarily lack a reasonable expectation of privacy for activities conducted out of doors in fields." for Clearly, the court defined drone flight as a public activity, lacking any privacy protection under the Fourth Amendment. However, there are exceptions such as indoor drone flight or flights at a designated drone park that are exempt from the Remote ID broadcast requirements. The exceptions do not define the Rule though, and the court found that the Rule's substance and requirements do not run up against Fourth Amendment prohibitions regarding law enforcement monitoring, surveillance, or disclosure of personally identifying information.

^{56.} *Id.* (quoting Nat'l Ass'n of Regul. Util. Comm'rs v. Fed. Energy Regul. Comm'n, 964 F.3d 1177, 1188 (D.C. Cir. 2020)).

^{57.} Id.

^{58.} Id. at 54.

^{59.} See id.

^{60.} Id. at 60.

^{61.} Id. at 61-62 (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

^{62.} See id.

^{63.} Id. at 58; Final Rule, supra note 2, at 4436.

^{64.} Brennan, 45 F.4th at 62-64.

1. The Remote ID Rule calls for installation, not monitoring by law enforcement

The court cited strong Fourth Amendment precedent holding that the presence of technology that could allow law enforcement monitoring does not automatically equate to actual law enforcement monitoring.⁶⁵ That precedent includes *United States v Karo*⁶⁶ and *United States v Knotts*,⁶⁷ together standing for the principle that the potential for law enforcement misuse is not equivalent to actual misuse.⁶⁸ The court found that the Remote ID rule similarly requires only the installation of broadcast equipment, without any involvement of governmental interception of broadcast signals.⁶⁹ It is worthy to note that the Remote ID rule contemplates law enforcement use "when necessary and relevant to a[n] FAA enforcement activity,"⁷⁰ subject to "all due process and other legal and constitutional requirements."⁷¹ The court dispensed with the installation issue without further analysis.

2. The characteristics of drone operations make governmental "dragnet" surveillance unlikely

The court found that drone flights are brief and occasional.⁷² Because the Remote ID rule requires broadcast of a signal only during flight,⁷³ the court reasoned that "[r]equiring 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."⁷⁴ The court distinguished the "limited, local, real-time information sharing," required by the Remote ID rule, from the longer term, more comprehensive data gathering found to be unconstitutional in *Carpenter* and *Jones*.⁷⁵ Specifically, 127 days of cell phone derived location data in *Carpenter*⁷⁶ and 28 days of GPS derived location data in *Jones*⁷⁷ versus "[a] drone system's real-time location data [that] says nothing qualitative about the nature of the location nor the operator's relationship to it (e.g. whether he is at his

^{65.} Id. at 62.

^{66. 468} U.S. 705 (1984).

^{67. 460} U.S. 276 (1983).

^{68.} Karo, 468 U.S. at 712; Knotts, 460 U.S. at 284-85.

^{69.} Brennan, 45 F.4th at 62.

^{70.} Id. at 54.

^{71.} *Id.* at 64; *Final Rule*, *supra* note 2, at 4433.

^{72.} Brennan, 45 F.4th at 62-63.

^{73.} Final Rule, supra note 2, at 4410 (codified at 14 C.F.R. § 89.110 (2023)).

^{74.} Brennan, 45 F.4th at 63.

^{75.} Id.

^{76.} Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

^{77.} United States v. Jones, 565 U.S. 400, 403 (2012).

home.)"⁷⁸ Practically, the Remote ID broadcast from a drone is not detectable beyond a distance of about a one-mile radius around the drone⁷⁹ making coordinated surveillance by law enforcement technically difficult, and the court noted the Remote ID rule itself does not contemplate the collection or storage of broadcast data for later governmental use.⁸⁰ Finally, the FAA has indicated that it would not record any broadcast data.⁸¹

3. The Remote ID rule limits access to personally identifying information

The court highlights the Remote ID rule's affirmative limitation protecting the revealing of personally identifying information through the use of an anonymous identifier,82 reasoning that "[t]he 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."83 A further limitation is the prohibition on anyone, other than the FAA, from using the serial number to match the drone's registration information, and limits that matching for reasons solely of airspace safety and security related to the drone's operation.⁸⁴ The court notes that additional layers of protection exist in the Privacy Act and other "Constitutional restrictions."85 The court found that although the Remote ID rule does not authorize law enforcement access to drone operators' personally identifying information, it does not prohibit it either.86 Because of the potential for future law enforcement misuse of the data in this context, the court explicitly left open the possibility of an asapplied challenge, even as it denied Brennan's facial challenge to the Remote ID rule.87

C. DRONE OPERATORS LACK ANY REASONABLE EXPECTATION OF PRIVACY OF THEIR DRONE SYSTEMS DURING FLIGHT

The court found Brennan failed to show the broadcast of data required by the Remote ID rule offends the Fourth Amendment in the "typically very public activity of drone piloting."88 Notwithstanding Petitioners' claim that

^{78.} Brennan, 45 F.4th at 63.

^{79.} *Id*.

^{80.} Id. at 63-64.

^{81.} Id. at 64; U.S. Dep't of Transp., Privacy Impact Assessment: Remote Identification of Unmanned Aircraft Final Rule (Remote ID Final Rule) 10 (2021).

^{82.} Brennan, 45 F.4th at 64; Final Rule, supra note 2, 4410, 4412.

^{83.} Brennan, 45 F.4th at 64.

^{84.} Id.

^{85.} Id.

^{86.} Id.

^{87.} Id. at 64-65.

^{88.} Id. at 64.

drone operators could operate a drone while inside a house and fly the drone in the house's curtilage, 89 the court equated this activity with public activity: "[d]rones fly in the open, and people ordinarily lack a reasonable expectation of privacy 'for activities conducted out of doors in fields."90 And even though the curtilage is afforded more Fourth Amendment protection than an open field, activities "conducted in the curtilage of a home, even behind a hedge or fence, if they may be viewed by 'naked eye observation'... from a public route or adjoining premises" are not so protected.91 The court linked the holding from California v. Ciraolo, 92 a landmark case allowing warrantless surveillance by aircraft, to aircraft flight itself.93 Whereas Ciraolo broadly concerned observation of the ground from aircraft in flight, the instant case broadly concerns observation of the aircraft itself in flight essentially the reverse of *Ciraolo*. 94 "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"95 to "ensure that even drone pilots shoulder the baseline responsibility of [safety]."96 Essentially, the court found the safety and security of people on the ground and other aircraft outweighs the privacy interests of drone operators.⁹⁷

IV. IMPACT

Beyond the narrow issue of drone operators' privacy rights, a larger issue remains unaddressed. That issue is the difference between public, navigable airspace and privately owned airspace, and the extent of the FAA's regulatory authority over privately owned airspace. Brennan claimed both constitutional and statutory overreach by the FAA in regulating low altitude airspace. Brennan framed this issue as a procedural matter, and the court dismissed his overreach argument as insignificant, holding that the "FAA adequately responded to significant comments." Therefore, all drone operators must comply with the Remote ID rule, no matter where the operation takes place.

^{89.} Brief of Petitioners, supra note 6, at 22-23.

^{90.} Brennan, 45 F.4th 48 at 61-62 (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

^{91.} *Id.* (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)) (citing United States v. Knotts, 460 U.S. 276, 281-82 (1983)).

^{92. 476} U.S. 207 (1986).

^{93.} See Brennan, 45 F.4th at 62.

^{94.} See generally Ciraolo, 476 U.S. at 207.

^{95.} Brennan, 45 F.4th at 60.

^{96.} Id.

^{97.} See id.

^{98.} Brief of Petitioners, supra note 6, at 49-51.

^{99.} Brennan, 45 F.4th at 71.

A. ALL DRONE OPERATORS MUST COMPLY WITH THE REMOTE ID RULE, EVEN THOSE FLYING IN PRIVATE AIRSPACE

The court found that the rights of people on the ground and others sharing the airspace outweighed the privacy rights of drone operators and upheld the Remote ID rule's burden on drone operators on this basis. 100 Despite the court acknowledging in its discussion a distinction between public, navigable airspace and privately owned airspace, the court did not find Petitioners' argument on the matter to be persuasive. Therefore, drone operators may very well be flying their drones in privately owned "superadjacent" 101 airspace very near the ground, but still must install and use the equipment required by the Remote ID rule. The only exceptions are enumerated in the Rule itself, which exempts drone flights that occur indoors and in FAA designated drone parks. 102

B. THE COURT DID NOT DISTINGUISH PUBLIC VERSUS PRIVATE AIRSPACE

The court tacitly acknowledged the issue of public versus private airspace in setting out the background of the case, discussing the reasons for the Remote ID rule, including drones "straying into *private* or sensitive areas." ¹⁰³ Further, the court cites to the United States Code empowering the FAA to "develop plans and policy for the use of the *navigable airspace*." ¹⁰⁴ Brennan raised the public versus private airspace issue as a procedural matter, asserting the FAA disregarded public comments regarding the "FAA's statutory and constitutional authority to regulate ... *non-navigable airspace*." ¹⁰⁵ Nonetheless, the court made little of this claim in the end, dispensing it, and others, by characterizing them as "frivolous." ¹⁰⁶ Further, only one paragraph earlier, the court described Brennan's efforts as attempting to distinguish "drone operations only within the 'navigable airspace' subject to FAA regulation, by instead purporting to apply throughout the 'airspace of the United States' which he views as more encompassing." ¹⁰⁷ Despite acknowledging multiple times in its opinion that

^{100.} See id. at 60.

^{101.} The United States Supreme Court in *United States v. Causby*, 328 U.S. 256, 265 (1946), defined "superadjacent airspace" as that airspace within the immediate reaches of the surface estate, but explicitly declined to define an upper limit of that super adjacent airspace.

^{102.} Brennan, 45 F.4th at 58-59.

^{103.} *Id.* at 55 (emphasis added).

^{104.} Id. at 56 (citing 49 U.S.C. § 40103(b)(1)) (emphasis added).

^{105.} Brief of Petitioners, *supra* note 6, at 15 (emphasis added).

^{106.} Brennan, 45 F.4th at 72.

^{107.} *Id.* (citations omitted); *see also* U.S.C. § 40103(a) (giving the FAA the authority to regulate "airspace of the United States"), (b)(1) (allowing the FAA to adopt policies for "the use of navigable airspace").

there is navigable airspace and there also is private, or non-navigable airspace, the court declined to make any distinction between public versus private airspace.

V. CONCLUSION

The court held that the Remote ID rule does not violate the Fourth Amendment on its face, and that the FAA met its procedural obligations required by the Administrative Procedures Act. All drone operators must comply with the Rule's requirements, even those operating in non-navigable, private airspace within the curtilage. The court acknowledged in its opinion the existence of both public, navigable airspace and private airspace but did not provide any further analysis or guidance. The question to what extent the FAA has regulatory authority over private, non-navigable airspace remains unresolved.