

PLANE-ARAZZI: BALANCING REMEDIES FOR CELEBRITIES TRACKED BY ADS-B WITH THE THREAT OF CENSORSHIP

“Man must rise above the Earth—to the top of the atmosphere and beyond—for only thus will he fully understand the world in which he lives.”

– Socrates

“Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”

– Louis Brandeis

“Everything is unprecedented until it happens for the first time.”

– Chesley “Sully” Sullenberger

INTRODUCTION

Since their rollout in 2008 and widespread adoption in the years since, Automatic Dependent Surveillance-Broadcast (ADS-B) transponders have made air travel both smarter and safer.¹ In 2024, anyone with a smartphone can download their plane tracking app of choice—made possible by crowdsourcing reception of ADS-B transmissions—and hold worldwide airspace in the palm of their hand.² However, the ADS-B rollout hasn’t been

1. See *Benefits*, FAA (Apr. 15, 2022), https://www.faa.gov/air_traffic/technology/equipadsb/capabilities/benefits [<https://perma.cc/78MV-UUEL>] (explaining the benefits of Equip ADS-B); Geneva Williams, Comment, *GPS for the Sky: A Survey of Automatic Dependent Surveillance-Broadcast (ADS-B) and Its Implementation in the United States*, 74 J. AIR L. & COM. 473, 490 (2009); see also Daniel Shoffet, Comment, *Drone Integration: A Pilot’s Solution to a Serious Entertainment Problem*, 33 J. INFO. TECH. & PRIV. L. 1 (2016) (advocating for regulation to require ADS-B receivers on drones).

2. Jacopo Prisco, *Inside Flightradar24, the Website That Tracks Every Plane in the Sky*, CNN (Aug. 25, 2022, 4:16 AM), <https://www.cnn.com/travel/article/flightradar24-flight-tracking-website/index.html> [<https://perma.cc/6CR8-AS69>]. See also *infra* Part I for additional information on how flight-aggregating applications collect and display ADS-B data.

ideal for one group of people: celebrities. The infamous “ElonJet” Twitter³ account, which published trips taken by Elon Musk’s private plane in real-time using ADS-B information, faced Musk’s ire and a suspension after a stalker allegedly used it to follow and harass his young son.⁴ One reporter has even suggested that Musk’s “motivation to ban the jet-tracking account was the primary driver behind [his] \$44 billion purchase [of Twitter].”⁵

Other celebrities, including Taylor Swift and Kylie Jenner, have faced criticism for emissions generated by their private flights as a result of the public’s access to their flight data.⁶ Flight tracking has also empowered amateur sleuths in celebrities’ criminal investigations—for example, following multiple law enforcement raids on Sean “Diddy” Combs’s properties, Diddy’s private plane generated much speculation as social media users tracked its flight path to a rumored escape.⁷ While these personalities have yet to take concrete legal action,⁸ the ADS-B tracking capability raises several questions about whether or not passengers have any

3. After Musk’s purchase of the company, Twitter officially rebranded to become X on July 23, 2023. See Saira Mueller, *Why Is X Still Called Twitter?*, CNN (Feb. 23, 2024, 4:00 PM), <https://www.cnn.com/2024/02/23/tech/twitter-x-rebrand-ccc/index.html> [https://perma.cc/PL4D-SAUJ]. Throughout this Note, “Twitter” refers to the company prior to the rebrand, while “X” refers to the company after the rebrand.

4. James Bickerton, *Elon Musk Claims ‘Stalker’ Targeted Car with Young Son Inside*, NEWSWEEK (Dec. 21, 2022, 1:28 PM), <https://www.newsweek.com/elon-musk-claims-stalker-targeted-car-young-son-inside-1767293> [https://perma.cc/62XY-FYR4]; see also Jess Weatherbed, *ElonJet Is Back on Twitter, but with a 24-Hour Delay*, THE VERGE (Dec. 23, 2022, 11:26 AM), <https://www.theverge.com/2022/12/23/23524060/twitter-elon-musk-jet-tracking-elonjet-elonjetnextday> [https://perma.cc/5JMT-K8V9].

5. Aidin Vaziri, *Elon Musk Bought Twitter to Block an Account Tracking His Private Jet, Book Reveals*, S.F. CHRON. (Feb. 12, 2024), <https://www.sfchronicle.com/tech/article/elon-musk-twitter-battle-bird-18663113.php> [https://perma.cc/ST86-7GUU]; see also KURT WAGNER, *BATTLE FOR THE BIRD: JACK DORSEY, ELON MUSK, AND THE \$44 BILLION FIGHT FOR TWITTER’S SOUL 159* (2024) (ebook) (“He didn’t love that Twitter allowed an account called @ElonJet that tracked the location of his private plane, and had even complained to [former Twitter CEO Parag] Agrawal about @ElonJet as recently as January 2022, right around the same time that he started buying Twitter stock.”).

6. See Allyson Chiu, *Celebrities Use Private Jets Excessively. It’s a Climate Nightmare.*, WASH. POST (Aug. 2, 2022, 8:22 PM), <https://www.washingtonpost.com/climate-environment/2022/08/02/taylor-swift-kylie-jenner-private-jet-emissions/> [https://perma.cc/QKT5-PUS8].

7. See Mike Bedigan, *Sean ‘Diddy’ Combs’ Private Jet Taken off Tracking App After Claims He Fled to the Caribbean Before Home Raids*, THE INDEP. (Mar. 26, 2024, 8:59 PM), <https://www.the-independent.com/news/world/americas/crime/sean-combs-diddy-private-jet-raids-b2519044.html> [https://perma.cc/ZA5H-5L7C]; see also David Goodhue & Jacqueline Charles, *Where’s Diddy? One Caribbean Nation Ruled Out*, MIA. HERALD (May 17, 2024, 3:30 PM), <https://www.miamiherald.com/news/local/community/miami-dade/miami-beach/article287086200.html> [https://perma.cc/RS4H-A8JQ].

8. However, some have threatened suit. Taylor Swift, after facing several close calls with stalkers and nonstop publicity surrounding her relationship with football player Travis Kelce, sent a cease-and-desist letter through her attorney to the owner of an account tracking her flights. Drew Harwell, *Taylor Swift Threatens Legal Action Against Student Who Tracks Her Jet*, WASH. POST (Feb. 6, 2024, 8:00 AM), <https://www.washingtonpost.com/technology/2024/02/06/taylor-swift-jet-tracking-legal-threat/> [https://perma.cc/LF9S-4GRQ] (“Swift’s attorney . . . [sent] a cease-and-desist letter saying Swift would ‘have no choice but to pursue any and all legal remedies’ if he did not stop his ‘stalking and harassing behavior.’”).

available legal remedies to shield their flight data and if flight tracking bots⁹ are protected under the First Amendment.

The Federal Aviation Administration (FAA)¹⁰ has started programs allowing aircraft owners to restrict dissemination of their flight information.¹¹ Elon Musk's enrollment¹² in these programs, however, did not deter ElonJet creator Jack Sweeney—who defiantly moved his live-tracking Musk-dedicated bot to the Instagram and Threads social media platforms after his ban from X and has since created additional bots for multiple celebrities, including Kim Kardashian, Mark Zuckerberg, and Jeff Bezos.¹³

Until the FAA's privacy programs evolve to outsmart persistent flight-tracking bot maintainers like Sweeney, celebrities seeking to protect their flight data have limited options to do so. The federal criminal cyberstalking penalty, 18 U.S.C. § 2261A(2), requires an intent to “kill, injure, harass, or intimidate” and cause another person either substantial emotional distress or to have a reasonable fear of death or serious bodily injury.¹⁴ The federal cyberstalking crime was enacted as part of the Violence Against Women Act of 2005, and it is primarily used in sextortion cases, domestic disputes,

9. For further discussion on flight tracking bots, see *infra* Part I.

10. The FAA regulates all of the United States' “civil aviation activities, including management of air traffic in U.S. airspace.” *Federal Aviation Administration*, U.S. DEP'T OF TRANSP. (May 2, 2018), <https://www.transportation.gov/briefing-room/safetyfirst/federal-aviation-administration> [<https://perma.cc/B4L9-H6TG>]. “[E]stablished by the Federal Aviation Act of 1958,” the FAA's mission “is to regulate civil aviation and U.S. commercial space transportation, maintain and operate air traffic control and navigation systems for both civil and military aircrafts, and develop and administer programs relating to aviation safety and the National Airspace System.” *Federal Aviation Administration*, FED. REG., <https://www.federalregister.gov/agencies/federal-aviation-administration> [<https://perma.cc/PNQ9-Q927>].

11. See *ADS-B Privacy*, FAA (Feb. 2, 2024) [hereinafter *ADS-B Privacy*], https://www.faa.gov/air_traffic/technology/equipadsb/privacy [<https://perma.cc/C7SY-E5WF>]; *Limiting Aircraft Data Displayed (LADD)*, FAA (Jan. 26, 2023) [hereinafter *LADD*], <https://www.faa.gov/pilots/ladd> [<https://perma.cc/E2D3-473S>].

12. Jason Koebler, *Emails Show SpaceX Bungled Elon Musk's Private Jet Privacy*, VICE (May 24, 2023, 12:48 AM), <https://www.vice.com/en/article/7kx8wa/emails-show-spacex-bungled-elon-musks-private-jet-privacy> [<https://perma.cc/D6LJ-HPTX>].

13. Jess Weatherbed, *The Elon Musk Private Jet Tracker Resurfaces on Threads and Immediately Goads Mark Zuckerberg*, THE VERGE (July 10, 2023, 8:26 AM), <https://www.theverge.com/2023/7/10/23789481/elon-musk-private-jet-tracker-threads-twitter-bot-elonjet> [<https://perma.cc/CVM9-NZHZ>].

14. 18 U.S.C. § 2261A(2). Interestingly, Taylor Swift's cease-and-desist letter invokes several elements of the cyberstalking penalty, alleging that Sweeney's accounts had caused “direct and irreparable harm, as well as emotional and physical distress,” forcing Swift “to live her life in a constant state of fear for her personal safety.” Koh Ewe, *Wrongful and Dangerous Actions Must Stop: Read the Full Cease-and-Desist Letter Taylor Swift's Lawyers Sent to Her Flight Tracker*, TIME (Feb. 7, 2024, 9:00 PM), <https://time.com/6692227/taylor-swift-cease-desist-letter-jack-sweeney-jet-tracker-emissions/> [<https://perma.cc/BU23-C92U>]. Swift's attorney further maintains that Sweeney's flight-tracking has become a “life-or-death matter.” *Id.*; see also Harwell, *supra* note 8 (describing Swift's cease-and-desist letter, which characterizes Sweeney's flight tracking as “stalking and harassing behavior”).

doxxing, and cyberbullying.¹⁵ Since flight data is public information and celebrities, as public figures, have a reduced expectation of privacy in certain matters, the criminal route would likely be feasible only in the most severe cases.¹⁶ Even when celebrities are targeted by traditional stalkers, courts—at least those limited by restrictions on bail and pretrial detention¹⁷—tend to play a game of ‘catch and release’ with seldom-deterred offenders.¹⁸

Absent criminal protections, people aiming to protect their flight data could seek out the civil route by suing for injunctive relief. However, this would lead them into the minefield of balancing the right to privacy with the First Amendment,¹⁹ which is further complicated by the fact that privacy is not generally recognized as an express right under U.S. constitutional law.²⁰ Currently, bots enjoy at least some form of First Amendment

15. *Cyberstalking: Two Federal Cases Illustrate the Consequences of Sextortion*, FBI (Oct. 30, 2018), <https://www.fbi.gov/news/stories/sentences-in-separate-cyberstalking-cases-103018> [<https://perma.cc/QHZ8-FWY4>].

16. *See infra* Section II.B. For an example of such a case, see also *Counterman v. Colorado*, 600 U.S. 66 (2023), holding that a state conviction for thousands of threats of violence against a celebrity violated the First Amendment because the state had not proved that the defendant recklessly disregarded “a substantial risk that [these] communications would be viewed as threatening violence.” *Id.* at 69.

17. For example, in New York, “[m]isdemeanors of assault, aggravated harassment, menacing, stalking, and more . . . do not qualify for money bail without the presence of another qualifying offense (e.g., violation of a protective order).” Hannah Gutenplan, Note, *A Fairer, Safer, and More Just System for All New Yorkers: Domestic Violence and New York Bail Reform*, 40 COLUM. J. GENDER & L. 206, 228 (2020); *see also* Tim McNicholas, *Taylor Swift’s Stalking Saga Highlights Vulnerabilities in System for Everyday New Yorkers*, CBS NEWS (Jan. 25, 2024, 6:13 PM), <https://www.cbsnews.com/newyork/news/taylor-swift-stalker-domestic-violence-restraining-orders/> [<https://perma.cc/GY6L-XYHM>] (discussing how laws restricting judges from “setting bail on certain offenses” allowed an alleged serial stalker to be released).

18. *See, e.g.*, John Miller & Celina Tebor, *Man Arrested Again Outside Taylor Swift’s Townhouse Less than 48 Hours After Prior Arrest There*, CNN (Jan. 23, 2024, 11:12 AM), <https://www.cnn.com/2024/01/23/us/taylor-swift-stalking-arrest-nyc/index.html> [<https://perma.cc/F75E-QDNR>]; Abbey White, *Drew Barrymore’s Alleged Stalker Arrested and Charged in New York*, HOLLYWOOD REP. (Aug. 24, 2023, 11:52 PM), <https://www.hollywoodreporter.com/news/general-news/drew-barrymore-alleged-stalker-chad-michael-busto-arrested-new-york-1235574423/> [<https://perma.cc/FW9R-AAKX>].

19. In libel actions, for example, “[t]he first amendment interest in free discussion of public issues clashes with individual reputational interests whenever the discussion of those issues includes libelous statements. To protect either interest completely is to abandon the other.” Eileen Carroll Prager, Note, *Public Figures, Private Figures and Public Interest*, 30 STAN. L. REV. 157, 157–58 (1977). “The reputational interests protected by libel law are really of two separate kinds: the interest in preserving one’s public good name and the interest in preserving one’s privacy.” *Id.* at 166–67.

20. *Cf.* NEIL RICHARDS, *INTELLECTUAL PRIVACY* 17 (2015) (discussing how, as “part of a wave of privacy anxiety sweeping the Gilded Age’s upper classes,” legal scholars “argued that the common law should protect a right to privacy,” in a manner that “was as brilliant as it was loose with the existing Anglo-American legal precedent, which did not really protect a right to privacy after all”).

protection²¹ while lawmakers and legal scholars are attempting to spell out exactly how much of it they deserve.²²

In this Note, I will more deeply explore the foundations of privacy law and their applications to flight data. I will further advocate that the public interest in tracking flight information outweighs celebrities' desires to keep their travels secret, especially as private air travel has an outsized impact on pollution²³ and flight data suppression programs have been used to shield criminal enterprises²⁴ and corruption.²⁵ Finally, I will discuss ways in which decisionmakers can appropriately balance legitimate privacy and safety interests with the public's right to know.

I. THE ASCENT OF ADS-B IN U.S. AVIATION AND RESULTING PRIVACY CONCERNS

Until the mid-2000s, U.S. aviation relied primarily on World War II-era radar technology, exacerbating air traffic congestion and safety concerns as the number of travelers—and as a result, aircraft in the sky—increased.²⁶ For decades, pilots relied on “eyesight and air traffic control radio communication to achieve ‘situation awareness,’ a mental picture of all surrounding aircraft.”²⁷ While high-quality training and dedication from pilots kept passengers safe, multiple near-misses and a few fatal crashes still occurred, resulting from confusion due to overwhelmed “human cognitive capabilities.”²⁸

Unlike the old system, ADS-B determines an airplane's position by using signals from orbiting satellites, and then broadcasts this position to nearby

21. Laurent Sacharoff, *Do Bots Have First Amendment Rights?*, POLITICO MAG. (Nov. 27, 2018), <https://www.politico.com/magazine/story/2018/11/27/bots-first-amendment-rights-222689/> [<https://perma.cc/RB8A-EC2V>].

22. See, e.g., Nathan Cortez & William Sage, *The Disembodied First Amendment*, 100 WASH. U. L. REV. 707 (2023).

23. See Oliver Milman, *A 17-Minute Flight? The Super-Rich Who Have ‘Absolute Disregard for the Planet.’* THE GUARDIAN (July 21, 2022, 5:00 PM), <https://www.theguardian.com/environment/2022/jul/21/kylie-jenner-short-private-jet-flights-super-rich-climate-crisis> [<https://perma.cc/B39Y-WAXK>].

24. See, e.g., J.K. Trotter, *Flight Data from Jeffrey Epstein's Private Jets Show a Lavish Travel Schedule as the Walls Closed in*, BUS. INSIDER (July 12, 2019, 4:36 PM), <https://www.businessinsider.com/jeffrey-epsteins-private-jet-flight-data-2019-7> [<https://perma.cc/EN3F-VRP5>] (“Epstein, however, ha[d] long taken advantage of a little-known federal policy that permits the owners of private jets to conceal their real-time movements from public view.”).

25. See Michael Grabell & Sebastian Jones, *Off the Radar: Private Planes Hidden from Public View*, PROPUBLICA (Apr. 8, 2010, 10:12 PM), <https://www.propublica.org/article/off-the-radar-private-planes-hidden-from-public-view-040810> [<https://perma.cc/3US5-UEU2>].

26. See Williams, *supra* note 1, at 473–75.

27. Thom Patterson, *Air Traffic Overhaul Hinges on ‘Human Factor.’* CNN (Mar. 9, 2011, 10:12 PM), <http://www.cnn.com/2011/TECH/innovation/03/09/nextgen.tech/index.html> [<https://perma.cc/29M7-EUEQ>].

28. *Id.*; see also *Mayday: System Breakdown* (Cineflix television broadcast June 10, 2009) (examining several mid-air collisions and ADS-B's possible impacts on air traffic safety).

aircraft and to ground-based relay stations, which transmit that information to air traffic control.²⁹ The FAA started implementing ADS-B as part of its NextGen program, formed as a result of the Vision 100—Century of Aviation Reauthorization Act of 2003, which “established the Joint Planning and Development Office to create a unified vision of what the U.S. National Airspace System (NAS) should deliver for the next generation and beyond.”³⁰

The FAA had officially been working to integrate ADS-B since NextGen’s creation; however, a tragic accident in 2006 further accelerated its pace. In August 2006, Comair Flight 5191 crashed in Lexington, Kentucky, killing forty-nine people.³¹ The National Transportation Safety Board (NTSB) in its investigation attributed the cause to pilot error, saying that the “crewmembers failed to recognize that they were initiating a takeoff on the wrong runway.”³² Further, the sole air traffic controller on duty at the time only had “two hours of sleep between shifts, and did not see the plane as it turned onto the wrong runway.”³³ In the aftermath, the FAA speculated that availability of “GPS-enabled airport surface maps in the cockpit might have averted” the disaster.³⁴

The FAA officially published Federal Regulations 14 C.F.R. §§ 91.225 and 91.227 in May 2010, mandating that, after January 1, 2020, all aircraft operating in airspace defined in Section 91.225 be equipped with an ADS-B system meeting the positional requirements defined in Section 91.227.³⁵ As of January 2024, over 166,000 aircraft are now outfitted with ADS-B transponders in compliance with these regulations.³⁶ ADS-B has undoubtedly made air travel safer and more efficient by “reduc[ing] the risk of runway incursions . . . [and] potential collisions” by providing “displays showing other aircraft in the sky” to pilots.³⁷

However, the new system has also raised concerns relating to cybersecurity. Some aviation security experts have expressed that

29. Patterson, *supra* note 27.

30. *NextGen Background*, FAA (Mar. 14, 2024), <https://www.faa.gov/nextgen/background> [<https://perma.cc/377S-TR7Y>].

31. Jane Davenport, *17 Years Later, Remembering Comair Flight 5191*, ABC 36 (Aug. 28, 2023), <https://www.wtvq.com/17-years-later-remembering-comair-flight-5191/> [<https://perma.cc/TWA5-8XQP>].

32. NAT’L TRANSP. SAFETY BD., NTSB/AAR-07/05, ATTEMPTED TAKEOFF FROM WRONG RUNWAY, COMAIR FLIGHT 5191, BOMBARDIER CL-600-2B19, N431CA, LEXINGTON, KENTUCKY, AUGUST 27, 2006, at 68 (2007).

33. Williams, *supra* note 1, at 479.

34. Patterson, *supra* note 27.

35. *Frequently Asked Questions*, FAA (April 15, 2022) [hereinafter *Equip ADS-B FAQ*], https://www.faa.gov/air_traffic/technology/equipadsb/resources/faq [<https://perma.cc/CW2R-83XN>].

36. *Current Equipage Levels*, FAA (Jan. 9, 2024), https://www.faa.gov/air_traffic/technology/equipadsb/installation/current_equipage_levels [<https://perma.cc/9PEZ-YL9N>].

37. *Equip ADS-B FAQ*, *supra* note 35.

“cyberattacks could impact part of the national air traffic control system . . . [and] the system becomes more vulnerable with the shift from radar control to GPS navigation” under NextGen.³⁸ Security risks involving the ADS-B system include “third-party spoofing (false aircraft position reports), malicious interference, and denial of service attacks.”³⁹ GPS jamming and spoofing in particular have recently caused disruptions to air travel amid ongoing military conflicts in the Baltics and the Middle East.⁴⁰ Israel, for example, in an effort to thwart attacks from Hezbollah, Iran, and other adversaries, has reportedly been “scrambling GPS signals over most of its northern airspace,”⁴¹ including those transmitted by civilian aircraft.⁴²

Potentially aggravating these concerns, anyone on the ground can set up an ADS-B receiver to capture aircraft signals in their vicinity.⁴³ This capability has led to the creation of numerous flight-tracking websites and mobile applications, powered by crowdsourcing data from a global community of aviation enthusiasts who link their ADS-B receivers into each platform’s network.⁴⁴ From there, people can create bots that scrape this data for a myriad of uses.⁴⁵

The most controversial of such uses involves setting up computerized tracking of public figures’ flights and posting live movements to social media, exemplified by programmer Jack Sweeney’s *ElonJet*. Creating an *ElonJet*-style bot is relatively simple with the right tools. Some have hypothesized that Sweeney found the registration number of Elon Musk’s plane from a fan’s website, and then set up a software program using

38. Stephen A. Wood, Dorothea (Thea) M. Capone & Mackenzie S. Wallace, *Aviation and Cybersecurity: An Introduction to the Problem and the Developing Law*, 46 THE BRIEF 38, 39 (2017).

39. David Tochen, *Blockchain Technology: A Solution in Search of a Problem—or a Revolution?*, 49 THE BRIEF 50, 55 (2019).

40. See Tommaso Lecca, *Airlines Report GPS Signal Jamming: Russia Gets the Blame*, POLITICO (Mar. 28, 2024, 4:06 PM), <https://www.politico.eu/article/airlines-flying-baltic-region-report-gps-signal-russia-gets-blame/> [<https://perma.cc/2DWN-RPF9>].

41. Matt Berg, *Israel’s Using Widespread GPS Tampering to Deter Hezbollah’s Missiles*, POLITICO (Oct. 23, 2023, 3:59 PM), <https://www.politico.com/news/2023/10/23/israels-gps-tampering-deter-hezbollahs-missiles-00123026> [<https://perma.cc/J3KT-F63A>].

42. See *id.*

43. See wondersmith rae, *How to Set up a Raspberry Pi ADS-B Flight Tracker for OSINT Investigation*, MEDIUM (Dec. 14, 2021), <https://wondersmithrae.medium.com/how-to-set-up-a-raspberry-pi-ads-b-flight-tracker-for-osint-investigation-927f9ad857f9> [<https://perma.cc/J9ZV-KDCJ>] (describing how to create an ADS-B receiver with only a Raspberry Pi, USB dongle, and an antenna); *Build Your Own ADS-B Receiver*, FLIGHTRADAR24, <https://www.flightradar24.com/build-your-own> [<https://perma.cc/57D6-2GS4>].

44. See *What Is the Exchange?*, ADS-B EXCH., <https://www.adsbexchange.com/what-is-the-exchange/> [<https://perma.cc/J4SB-AUWN>]; *An Introduction into ADS-B*, FLIGHTRADAR24, <https://www.flightradar24.com/blog/ads-b/> [<https://perma.cc/3WTE-EW8G>].

45. For example, tracking flight progress for friends, loved ones, and others; analyzing airline performance by route; or identifying sources of GPS signal interference.

Application Programming Interfaces (APIs)⁴⁶ to scrape publicly available flight data from tracking websites and post automated updates to social media accounts.⁴⁷ Sweeney also maintains a GitHub repository, plane-notify, which users can download and run to unleash their own flight tracking bots into cyberspace.⁴⁸

Several flight tracking aggregators have taken measures to curb this behavior. Flightradar24—one of the most popular flight-tracking applications⁴⁹—blocks certain flight information. Despite predominantly relying on its network of volunteer ADS-B receiver operators, “Flightradar24 cross-references its ground-based receivers with data . . . from the [FAA],” which means that it “must agree to abide by FAA rules that let aircraft owners request their information be removed from public websites.”⁵⁰ In contrast, ADS-B Exchange, another aggregator, does not use FAA data,⁵¹ allowing it to provide what it describes as “an unfiltered, uncensored window into global aerial movements.”⁵²

The FAA has devised two primary programs to protect flight data: the Limiting Aircraft Data Displayed (LADD) Program and the Privacy ICAO⁵³ Aircraft Address (PIA) Program. LADD was created to implement the “Right to Privacy When Using Air Traffic Control System” established in the 2018 HR 254 FAA Reauthorization Bill, Section 566—which appeared

46. For a definition of API, see John A. Rothchild, *Developments in Copyright and Trademark Law*, 77 BUS. LAW. 305, 305 (2021) (“[An API is comprised of] ready-made routines that software developers [can] incorporate[] . . . into their own programs . . . [to] save them the effort they would otherwise need to expend to code standard and relatively low-level functions.”).

47. See Victoria Angelova, *How a College Student Was Able to Track Elon Musk’s Private Jet Movements by Simply Using a Few APIs*, APILAYER (Feb. 17, 2022), <https://blog.apilayer.com/how-a-college-student-was-able-to-track-elon-musks-private-jet-movements-by-simply-using-a-few-apis/> [<https://perma.cc/RSA4-BUVA>].

48. Jxck-S, *Plane-Notify*, GITHUB, <https://github.com/Jxck-S/plane-notify> [<https://perma.cc/7SEQ-7GX8>].

49. See Prisco, *supra* note 2.

50. Wilfred Chan, *From Celebrity Jets to Pelosi’s Taiwan Trip, Flight Trackers Are the Sleeper Hit of the Summer*, THE GUARDIAN (Aug. 4, 2022, 1:00 PM), <https://www.theguardian.com/world/2022/aug/03/flight-trackers-flightradar24-ads-b-exchange> [<https://perma.cc/B7ZG-QLJ6>].

51. *Id.*

52. See *What Is the Exchange?*, *supra* note 44. However, ADS-B Exchange was purchased by JetNet LLC in 2023, stoking fear among aviation enthusiasts that the aggregator “might cave to requests from celebrities and others to yank their private-jet information off its website.” Grace Kay & Taylor Rains, *The College Student Who Tracks Elon Musk’s Private Jet Is Launching His Own Flight-Tracking Website*, BUS. INSIDER (Feb. 7, 2023, 5:11 PM), <https://www.businessinsider.com/student-who-tracks-elon-musk-jet-launching-own-website-2023-2> [<https://perma.cc/Y2TU-A7YK>]. This led Sweeney to launch his own competing jet-tracking website, TheAirTraffic. *Id.*

53. ICAO is an acronym for the International Civil Aviation Organization, a United Nations (UN) agency that coordinates air traffic between the UN’s 193 member countries. See *Acronyms and Abbreviations*, ICAO, https://www.icao.int/EURNAT/Documents/ECHO/Doc_8973-12_abbreviations.pdf [<https://perma.cc/VTB7-MSER>]; *About ICAO*, ICAO, <https://www.icao.int/about-icao/Pages/default.aspx> [<https://perma.cc/RWZ6-GSVH>].

as a note in Title 49 of the United States Code.⁵⁴ The program has constrained flight trackers that use FAA data, like Flightradar24, by “provid[ing] aircraft owners the ability to have their flight data filtered from distribution via the FAA System Wide Information Management (SWIM) data feed or filtered from public display by web sites that participate in the program.”⁵⁵

Yet, LADD cannot prevent independent aggregators from displaying unfiltered data. Therefore, the FAA also started the PIA program to allow aircraft owners to request alternate, temporary ICAO aircraft addresses that are not assigned to owners in the Civil Aviation Registry.⁵⁶ This assignment of temporary codes, in theory, “limit[s] the extent to which . . . aircraft can be quickly and easily identified by non-U.S. government entities, while ensuring there is no adverse effect on [air traffic control] services.”⁵⁷ However, in practice, PIA is still running years behind schedule. While the FAA originally planned to transfer the program to a third party in 2020, the agency was still maintaining PIA as recently as June 2023, and has refused to comment on the number of issues users have experienced in “the interest of privacy.”⁵⁸ Despite the FAA’s silence, experts are not convinced of the program’s efficacy, with some expressing that it “isn’t working because not enough aircraft are using it . . . and jet owners don’t change their fake codes frequently enough.”⁵⁹ Epitomizing the issues plaguing the program, a Freedom of Information Act (FOIA) Request revealed that Elon Musk enrolled his jet into PIA, but failed to implement it properly and sought help in the midst of his struggles with ElonJet.⁶⁰ After this experience, Musk temporarily gave up on hiding his flight information through the FAA in August 2022—but reenrolled in the program in June 2024 after the passage of the FAA Reauthorization Act of 2024.⁶¹

54. *LADD*, *supra* note 11; *see also* 49 U.S.C. § 44103 note (Right to Privacy When Using Air Traffic Control System), *repealed by* FAA Reauthorization Act of 2024, Pub. L. No. 118-63, § 803.

55. *LADD*, *supra* note 11.

56. *See ADS-B Privacy*, *supra* note 11.

57. *Id.*

58. Rebecca Heilweil, *FAA Aircraft Privacy Program Transition Is Running Years Behind*, FEDSCOOP (June 21, 2023), <https://fedscoop.com/faa-aircraft-privacy-program-transition-is-running-years-behind/> [<https://perma.cc/ND7X-G4G7>].

59. Jeremy Bogaisky, *Elon Musk May Have Given Up on Privacy for His Jet Travels, but Taylor Swift Hasn't*, FORBES (Oct. 25, 2023, 6:30 AM), <https://www.forbes.com/sites/jeremybogaisky/2023/10/25/elon-musk-may-have-given-up-on-privacy-for-his-jet-travels-but-taylor-swift-hasnt/?sh=7d2471225fb2> [<https://perma.cc/5CWW-GMPM>].

60. Koebler, *supra* note 12.

61. Grace Kay & Taylor Rains, *Elon Musk Appears to Have Given Up on Trying to Camouflage His Private-Jet Travels with an FAA Program Used by Jeff Bezos and Taylor Swift*, BUS. INSIDER (Oct. 28, 2023, 5:07 AM), <https://www.businessinsider.com/elon-musk-appears-no-longer-masking-private-jet-tracking-pia-2023-10> [<https://perma.cc/R3BZ-5QMN>]; Taylor Rains & Grace Kay, *Elon Musk Is Cloaking His Jet Travels Again*, MSN (July 12, 2024, 4:00 PM), <https://www.msn.com/en>

In the FAA Reauthorization Act of 2024, Congress repealed Section 566, adding in its place a new section in the United States Code explicitly dedicated to data privacy.⁶² To be codified as 49 U.S.C. § 44114 (Section 44114), the new provision will require the FAA, (1) upon the request of a private owner or operator, to withhold the requester’s aircraft registration number and “other similar identifiable data or information, except for physical markings required by law, . . . from any broad dissemination or display . . . for . . . noncommercial flights”;⁶³ (2) upon the request of a private owner or operator, “withhold from broad dissemination or display by the FAA” the requester’s “personally identifiable information”;⁶⁴ and (3) “establish a program for aircraft owners and operators to apply for a new ICAO aircraft identification code” where applicants must “attest to a safety or security need” to receive a new code.⁶⁵

While this provision could provide enhanced privacy for private flyers, any major advances will likely take time to get off the ground—especially considering the ongoing struggles facing LADD and PIA.⁶⁶ Therefore, private aircraft owners, operators, and passengers seeking protection for their flight data may continue to be left to navigate a complicated web of privacy rights and restrictions in the legal system until the FAA fully implements Section 44114.

-ie/news/techandscience/elon-musk-is-cloaking-his-jet-travels-again/ar-BB1pRabK [https://perma.cc/QB87-JG8U].

62. See Andrew Paul, *Tracking Private Jets Just Got Much Harder*, POPULAR SCI. (May 23, 2024, 2:25 PM), <https://www.popsoci.com/technology/tracking-private-jets/> [https://perma.cc/M5W5-TQXL]; FAA Reauthorization Act of 2024, Pub. L. No. 118-63, § 803.

63. FAA Reauthorization Act of 2024 § 803.

64. *Id.* Under the new law,

[t]he term ‘personally identifiable information’ means . . . (A) the mailing address or registration address of an individual; (B) an electronic address (including an email address) of an individual; or (C) the telephone number of an individual. (D) the names of the aircraft owner or operator, if the owner or operator is an individual.

Id.

65. *Id.*

66. Some ADS-B enthusiasts have expressed doubt that the new law’s provisions—even if implemented perfectly—will prevent ADS-B tracking. For example, in criticizing the law, Sweeney asserted that “[a] FOIA request is not broad dissemination, . . . [and] other sources of this data exist not via registry or not via FAA. . . . The only proper solution [for] privacy in the ADS-B era . . . is reducing access to ADS-B or encrypting ADS-B.” Jack Sweeney (@Jxck_Sweeney), X (May 27, 2024, 11:44 AM), https://x.com/jxck_sweeney/status/1795133872226566352?s=46&t=GIQCOHshD3yN5O8UGwofJA [https://perma.cc/5D4U-YKLF].

II. UNDERSTANDING THE CURRENT LEGAL LANDSCAPE FOR FLIGHT-TRACKING BOTS

A. *Privacy in U.S. Airspace*

In the United States, the federal Constitution does not explicitly protect a right to privacy, unlike many jurisdictions abroad.⁶⁷ While prior Supreme Courts have implied such a right,⁶⁸ at least one originalist member of the current Court appears to favor shifting away from that implication,⁶⁹ but the Court itself has not taken such a step yet.⁷⁰ The right to privacy, or the “right to be let alone,” was first widely introduced in the U.S. legal community by Samuel D. Warren and Louis Brandeis in their famed law review piece *The Right to Privacy*.⁷¹ Partially motivated by Warren and Brandeis’s desires to protect their own high-class lives from the prying eyes of the yellow press,⁷² the article served as a catalyst for the development of privacy protections in the common law.⁷³

Throughout much of the 20th century, privacy rights were primarily protected under tort law. Scholar William Prosser classified the governing privacy theories into four distinct torts: intrusion into private affairs, public disclosure of private facts, publicity placing another in a false light, and

67. In Europe, for example, privacy enjoys several layers of safeguards, including the European Convention on Human Rights (ECHR), Charter of Fundamental Rights of the European Union, and General Data Protection Regulation (GDPR). See Y.B. EUR. CONV. ON H.R. art. 8 (1950); Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. (C 364) 1, 10; Council Regulation 2016/679, 2016 O.J. (L 119) 1. This higher status does not eliminate nuance, however, and the highest European courts have regularly found the public interest to outweigh privacy rights in certain situations. See, e.g., Axel Springer AG v. Germany, Eur. Ct. H.R. at 15–20 (2014).

68. See *Griswold v. Connecticut*, 381 U.S. 479, 484–86 (1965) (holding that specific guarantees in the Bill of Rights created “zones of privacy” that protected contraceptive use); *Whalen v. Roe*, 429 U.S. 589 (1977) (recognizing a right to information privacy but finding that a New York prescription monitoring program did not violate it); *Lawrence v. Texas*, 539 U.S. 558 (2003) (protecting a right to participate in consensual, private sexual acts).

69. See *Dobbs v. Jackson Women’s Health Org.*, 597 U.S. 215, 332 (2022) (Thomas, J., concurring) (“[W]e should reconsider all of this Court’s substantive due process precedents, including *Griswold*, *Lawrence*, and *Obergefell*.”).

70. See *id.* at 290 (majority opinion) (“Nothing in this opinion should be understood to cast doubt on precedents that do not concern abortion.”).

71. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). After his appointment to the Supreme Court, Justice Brandeis again invoked the “right to be let alone” in a famous dissent. See *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (“The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”), *overruled by Katz v. United States*, 389 U.S. 347 (1967).

72. See RICHARDS, *supra* note 20, at 16–17 (“[E]lites like the Warrens felt the threat to their social position posed by a new generation of newspaper reporters. . . . Encouraged by [his wife] Mabel, Warren sought out Brandeis to write an article about the excesses of the press and the need for a legal right to privacy.”).

73. See WILLIAM MCGEVERAN, *PRIVACY AND DATA PROTECTION LAW* 113 (2d ed. 2023).

appropriation of another's name or likeness.⁷⁴ These formulations were later adopted in the second *Restatement of Torts*⁷⁵ and served as the foundation for many cases imposing liability for privacy violations.⁷⁶ However, protections under tort law have limits—particularly when certain information is “newsworthy”—or is of “legitimate concern to the public.”⁷⁷ In these cases, the First Amendment looms large, as courts fear censoring expressly-protected speech by elevating implicitly-protected privacy.⁷⁸

As a result, at least ten states have enshrined rights to privacy in their constitutions.⁷⁹ The people of California led the push for more privacy protections, amending the California Constitution in 1972 to “add ‘privacy’ to the list of ‘inalienable rights’ guaranteed by Article 1, Section 1”⁸⁰ This provision is highly relevant to celebrities seeking to assert privacy rights, including those regarding flight data, as California is one of the primary centers of the entertainment industry—requiring many celebrities to either live in or commute to the state regularly.⁸¹ However, critics have argued that even these explicit protections are inadequate,⁸² and no celebrity to date appears to have brought an action under these state provisions to protect their flight data.⁸³

74. See generally William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

75. RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D, 652E, 652C (AM. L. INST. 1977).

76. See, e.g., *Anderson v. Mergenhagen*, 642 S.E.2d 105 (Ga. Ct. App. 2007) (intrusion); *Y.G. v. Jewish Hosp. St. Louis*, 795 S.W.2d 488 (Mo. Ct. App. 1990) (publicity); *Welling v. Weinfeld*, 866 N.E.2d 1051 (Ohio 2007) (false light); *Pavesich v. New Eng. Life Ins. Co.*, 50 S.E. 68 (Ga. 1905) (appropriation).

77. See *Haynes v. Alfred A. Knopf, Inc.*, 8 F.3d 1222 (7th Cir. 1993) (holding a book publisher did not invade the plaintiff's privacy by publishing details about the plaintiff's marital life that related to the book's newsworthy social theme); see also *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975) (finding that criminalizing the release of a murder victim's name was unconstitutional under the First Amendment).

78. See *Cox*, 420 U.S. at 492–93 (“There is no special perquisite of the judiciary which enables it, as distinguished from other institutions of democratic government, to suppress, edit, or censor events which transpire in proceedings before it.” (quoting *Craig v. Harney*, 331 U.S. 367, 374 (1947))).

79. See FRANK DOUMA & JORDAN DECKENBACH, *THE IMPLICATIONS OF CURRENT AND EMERGING PRIVACY LAW FOR ITS 9* (2008).

80. J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 328 (1992).

81. See Bruce R. Bailey, *Privacy and Publicity Rights of Athletes and Celebrities in California*, 25 INT'L LEGAL PRAC. 53, 53 (2000).

82. See Chassen Palmer, Note, *Celebrity Privacy: How France Solves Privacy Problems Celebrities Face in the United States*, 50 CAL. W. INT'L L.J. 245, 254–63 (2019) (discussing “[f]ailure[s]” of California state law and U.S. federal law to protect celebrities).

83. Instead, they have used other methods, like “ma[king] a deal . . . to give . . . a lifetime of business advice to stop tracking . . . travel on Twitter” (Mark Cuban), “renting private planes” (Tim Cook, Bernard Arnault), “switch[ing] out . . . private jet[s]” (Mark Zuckerberg), and enrolling in FAA programs (Drake, Travis Scott, Donald Trump, and others). Taylor Rains & Grace Kay, *How Elon Musk, Donald Trump, Taylor Swift, and Others Are Trying to Dodge Jet Tracking*, BUS. INSIDER (Dec. 18, 2022, 8:13 AM), <https://www.businessinsider.com/how-celebrities-like-elon-musk-taylor-swift-dodge-jet-tracking-2022-11> [<https://perma.cc/HU9D-F8FM>].

In the administrative space, the Department of Transportation (DOT) regularly “investigate[s] complaints and take[s] action against airlines and ticket agents for unfair or deceptive practices,”⁸⁴ such as when airlines or ticket agents mishandle personal information collected from passengers. Currently, the DOT appears to primarily target these actions against larger passenger airlines; however, private flyers may be able to file complaints for particularly egregious flight data breaches caused by charter companies or airports.⁸⁵

B. Statutory Protections Against Cyber Harassment

In addition to private rights of action, several statutory frameworks, both at the federal and state level, criminalize invasions of privacy that amount to cyberstalking, also known as cyber harassment. Currently, forty-nine out of fifty states in the U.S. have implemented laws against cyberstalking.⁸⁶ Additionally, the federal government enacted its own provision, 18 U.S.C. § 2261A, which generally prohibits using electronic communications or the mail to intentionally cause substantial emotional distress to another person, or to place another person in reasonable fear of death or serious bodily injury to persons or certain animals.⁸⁷

However, the bar prosecutors must clear to obtain convictions under both state and federal law for cyberstalking and other forms of harassment is exceptionally high when defendants raise First Amendment claims. This is exemplified by the Supreme Court’s ruling in *Counterman v. Colorado*,⁸⁸ where the Court evaluated a defendant’s convictions for stalking and harassment under Colorado state law. In *Counterman*, “the Court held that the First Amendment requires proof that the defendant subjectively understood the threatening nature of his communications. The Court further held that recklessness is the minimum *mens rea* for a criminal conviction based on threats.”⁸⁹ Additionally, when they faced First Amendment

84. *Air Consumer Privacy*, U.S. DEP’T TRANSP. (Mar. 25, 2024), <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy> [<https://perma.cc/7GHJ-YHYT>].

85. For an example of such a breach, see Waqas, *Hackers Leak 2.5M Private Plane Owners’ Data Linked to LA Intl. Airport Breach*, HACKREAD (Feb. 23, 2024), <https://www.hackread.com/hackers-leak-private-plane-owners-data-la-airport-breach/> [<https://perma.cc/SYC3-5V95>].

86. See Natasha N. Phidd, Note, *A Call of Duty to Counterstrike: Cyberharassment and the Toxic Gaming Culture Plaguing Female Gamers and Developers*, 25 WM. & MARY J. RACE GENDER & SOC. JUST. 461, 470 (2019).

87. See *id.* at 466; 18 U.S.C. § 2261A.

88. 600 U.S. 66 (2023).

89. Joseph Palmer, *When Does Online Speech Become a Federal Crime?*, 71 DEP’T JUST. J. FED. L. & PRAC. 77, 78 (2023) (citing *Counterman*, 600 U.S. at 78–80). One scholar has argued that this “heightened *mens rea* requirement gives law enforcement further reason to dismiss reports of cyber gender abuse as acceptable behavior . . . [by] ‘immuniz[ing] stalkers who are untethered from reality’

challenges to the federal cyberstalking law, some courts interpreted the words “‘harass’ or ‘intimidate’ to limit the statute to unprotected speech.”⁹⁰

In their efforts to silence Sweeney, multiple celebrities have invoked elements of cyberstalking laws, particularly by accusing him of causing substantial emotional distress and fears of death or serious bodily injury by posting their live movements on social media.⁹¹ However, the aircraft registration information Sweeney has used to identify and track famous jets is “available to the public upon request”⁹² as of May 2024, and courts have been hesitant to sustain cyberstalking prosecutions and protective injunctions based on a defendant’s posting of public information.⁹³ Ironically, Sweeney claimed that *he* had received death threats from Taylor Swift’s fans because of his flight-tracking, which, if true, could make his case for protection under current cyberstalking laws stronger than the lawsuits Swift and Musk have warned they may bring against him.⁹⁴

However, courts on occasion have recognized a privacy interest in information that is publicly available but not easily accessible—or

and ‘allow[ing] devious stalkers to escape accountability by insisting they meant nothing by their harmful statements.’” Danielle Keats Citron, *The Continued (In)visibility of Cyber Gender Abuse*, 133 *YALE L.J.F.* 333, 363 (2023) (quoting Transcript of Oral Argument at 50, *Counterman v. Colorado*, 600 U.S. 66 (2023) (No. 22-138)).

90. Palmer, *supra* note 89, at 82 (citing *United States v. Yung*, 37 F.4th 70, 77–81 (3d Cir. 2022); *United States v. Ackell*, 907 F.3d 67, 76–77 (1st Cir. 2018)).

91. See Ewe, *supra* note 14 (describing cease-and-desist letter sent by Taylor Swift’s legal team, which attributed Sweeney’s jet-tracking as the cause of “emotional and physical distress”); Elon Musk (@elonmusk), TWITTER (Dec. 14, 2022, 6:48 PM), <https://twitter.com/elonmusk/status/1603190155107794944?s=20&t=vi1AkQM8orj1hHL-Uc5TsQ> [<https://perma.cc/RW9B-E9HX>] (alleging Sweeney “supported harm to [his] family”).

92. *Aircraft Registration*, FAA (Nov. 8, 2023), https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/about_aircraft_records [<https://perma.cc/H5AC-WNSP>]. However, Section 44114 will dramatically limit the public’s access to aircraft registration information, as the FAA will be required to “withhold[] the registration number and other similar identifiable data or information . . . from any broad dissemination or display . . . for the noncommercial flights of [a requesting] owner or operator.” FAA Reauthorization Act of 2024, Pub. L. No. 118-63, § 803.

93. See, e.g., *United States v. Cook*, 472 F. Supp. 3d 326, 335 (N.D. Miss. 2020) (“Certainly, sharing public information, while potentially offensive and disagreeable, does not rise to the level of a true threat.”); *Logue v. Book*, 297 So. 3d 605, 618–19 (Fla. Dist. Ct. App. 2020) (“Claims of threatening speech or harassing action are actionable if the speaker threatens, harasses or intimidates, and intended targets would reasonably perceive that intent. Merely posting public information, or potentially embarrassing and annoying content, without more, is not conduct within the stalking statute . . .”).

94. According to Sweeney, “[t]hey’re keyboard warriors, but that’s pretty much it. There’s someone [who] said, ‘I hope you get brutally murdered yourself,’ and they messaged me that, and it’s like these people, you can’t really respect their opinion because they don’t know how technology works.” Emma Parry & Chris White, *JEFF OFF: Taylor Swift’s Private Jet ‘Stalker’ Says Jeff Bezos Is Now Taking Aim at Him but Vows ‘Bullying Won’t Stop Me.’* U.S. SUN (Mar. 1, 2024, 6:14 PM), <https://www.the-sun.com/news/10546138/taylor-swifts-private-jet-stalker-jeff-bezos-bullying/> [<https://perma.cc/D5FK-55QH>]. While Sweeney does not appear to be fazed by the death threats, he would likely still receive protection under at least the federal cyberstalking penalty, which only requires that such threats “would be *reasonably expected to cause* substantial emotional distress.” 18 U.S.C. § 2261A(2)(B) (emphasis added).

“practically obscure.”⁹⁵ For example, in *United States Department of Justice v. Reporters Committee for Freedom of the Press*,⁹⁶ the Supreme Court held that the disclosure of a Federal Bureau of Investigation (FBI) rap sheet’s contents to a third party was prohibited under FOIA because the disclosure “could reasonably be expected to constitute an unwarranted invasion of personal privacy” within the meaning of one of the act’s exemptions.⁹⁷ Therefore, especially as Section 44114 threatens to further impede the public’s ability to access private flyers’ flight information, celebrities may be able to successfully invoke practical obscurity in their efforts to quash tracking by hobbyists like Sweeney.

C. *Speech, Bots, and the Public Interest*

In conflict with certain privacy rights and anti-harassment protections lies the right to freedom of expression.⁹⁸ First Amendment law in the United States progressed almost in parallel with privacy law in the 20th century—and was largely developed, somewhat ironically, by Justice Louis Brandeis.⁹⁹ In the new millennium, courts have faced growing challenges in defining its scope as technology has advanced to increase the average person’s ability to communicate.¹⁰⁰

95. See David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. ILL. L. REV. 1385, 1387 (2017). “‘Practical obscurity’ refers to the idea that even information that is publicly available can still have private attributes if it is difficult to access, find, or contextualize.” *Id.* at 1387 n.3 (citing Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 21 (2013)).

96. 489 U.S. 749 (1989).

97. *Id.* at 751, 779 (quoting 5 U.S.C. § 552(b)(7)(C)).

98. But see RICHARDS, *supra* note 20, at 95.

Instead of being conflicting values, privacy and speech can instead be mutually supportive. In fact, . . . a certain kind of privacy is essential . . . [for] freedom of expression. This kind of privacy is different from tort privacy. Let’s call it “intellectual privacy.”

. . . Essentially, it’s . . . a zone of protection that guards our ability to make up our minds freely. More formally, intellectual privacy is the protection from surveillance or unwanted interference by others when we are engaged in the processes of generating ideas and forming beliefs—when we’re thinking, reading, and speaking with confidants before our ideas are ready for public consumption.

Id.

99. See *id.* at 30–40.

100. See *Lindke v. Freed*, 601 U.S. 187 (2024) (holding that a public official who blocks someone from commenting on the official’s social media page engages in state action only if the official has actual authority to speak on behalf of the state on a particular matter and they purport to exercise that authority in the relevant posts); *Moody v. NetChoice, LLC*, 144 S. Ct. 2383 (2024) (vacating two judgments and remanding their cases because the Fifth and Eleventh Circuits did not conduct a proper analysis of the facial First Amendment challenges to Texas and Florida laws regulating internet platforms).

Following two infamous elections riddled with misinformation spewed by social media bots,¹⁰¹ legal scholars are now grappling with how to fit automated “speakers” into First Amendment jurisprudence. Some have argued that “[b]ots represent a new form of communication” and that regulations targeting them “implicate[] core free speech concerns.”¹⁰² Others have challenged this, questioning whether anyone’s “speech interests . . . are furthered by [certain] types of automated communication.”¹⁰³

Meanwhile, few legislatures have taken action to regulate bots. However, recent legislation passed by California¹⁰⁴ and Texas,¹⁰⁵ as well as mounting concerns about the impact of generative AI,¹⁰⁶ signal that government leaders may implement new measures to curb bots’ mostly free reign on the internet.

While many well-meaning actors are flailing over how to control automated misinformation, others with more insidious motives have set their sights on restricting truthful bots: flight-trackers. The Saudi government, irked by aggregators like “Dictator Alert,”¹⁰⁷ reportedly attempted to “push international aviation regulators to forbid or prevent the

101. See Sacharoff, *supra* note 21; AJ Vicens, *Researchers Say They’ve Uncovered a Massive Facebook Bot Farm from the 2020 Election*, MOTHER JONES (May 10, 2021), <https://www.motherjones.com/politics/2021/05/facebook-bot-farm/> [<https://perma.cc/836N-GCGT>].

102. Madeline Lamo & Ryan Calo, *Regulating Bot Speech*, 66 UCLA L. REV. 988, 1028 (2019). Abroad, a Canadian small claims court similarly seemed to afford bot speech some weight, finding that Air Canada was obligated to provide a discount promised by its AI chatbot even though the airline did not actually offer such a discount. *Moffatt v. Air Canada*, 2024 BCCRT 149, ¶ 27 (Can.) (“It should be obvious to Air Canada that it is responsible for all the information on its website. It makes no difference whether the information comes from a static page or a chatbot.”).

103. Cortez & Sage, *supra* note 22, at 723. Cortez and Sage in particular question whether “regulating search engines, robocallers, robotraders, and social media bots compromise[s] free speech simply because they perform some communicative function.” *Id.*

104. CAL. BUS. & PROF. CODE §§ 17940–43 (West 2024). § 17941(a) provides in relevant part:

It shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot.

105. Jayme Lozano Carver, *After Taylor Swift Eras Tour Glitch, Texas Bans Bots That Buy Concert Tickets*, TEX. TRIB. (May 23, 2023, 1:00 PM), <https://www.texastribune.org/2023/05/23/texas-concert-bot-law-taylor-swift/> [<https://perma.cc/3YK9-PMF8>].

106. See Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023) (“Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.”).

107. Amar Toor, *This Twitter Bot Is Tracking Dictators’ Flights in and out of Geneva*, THE VERGE (Oct. 13, 2016, 4:24 AM), <https://www.theverge.com/2016/10/13/13243072/twitter-bot-tracks-dictator-planes-geneva-gva-tracker> [<https://perma.cc/K932-A6KL>].

public dissemination of ADS-B data.”¹⁰⁸ In a more severe move, the Chinese government allegedly confiscated ADS-B receivers in its territory and banned Flightradar24 from mobile app stores, citing “national security concerns.”¹⁰⁹

These restrictions raise alarms over the public’s interest in valuable information provided by automated flight-tracking. One of the most glaring issues is private aviation’s outsized impact on carbon emissions—as “private jets generally carry few passengers for shorter distances, making them five to fourteen times more polluting than commercial planes, per passenger.”¹¹⁰ In the financial world, even in the early days of flight tracking, the Securities and Exchange Commission (SEC) used flight records to investigate companies for failing to disclose certain executive perks.¹¹¹ Crowdsourced data has also been used to investigate plane crashes within hours, especially in regions where information is tightly controlled.¹¹² Further, flight tracking can help monitor government surveillance¹¹³ and criminal enterprises, like drug lords’ “narco-planes”¹¹⁴ and human trafficking.¹¹⁵

108. Justin Ling, *The Flight Tracker that Powered @ElonJet Just Took a Left Turn*, WIRED (Jan. 27, 2023, 7:00 AM), <https://www.wired.com/story/ads-b-exchange-jetnet-sale/> [<https://perma.cc/UQ5Q-M3E3>].

109. Josh Ye & Danny Lee, *China’s Crackdown on Flight-Tracking Devices Leaves Companies and Hobbyists Frustrated*, S. CHINA MORNING POST (Nov. 12, 2021, 10:00 PM), <https://www.scmp.com/tech/policy/article/3155895/chinas-crackdown-flight-tracking-devices-leaves-companies-and-hobbyists> [<https://perma.cc/53D6-A2P5>]; see also Zhang Tong, *China Targets Devices It Says Are Used to Send Flight Data to ‘Foreign Entities.’* S. CHINA MORNING POST (Jan. 6, 2024, 8:00 PM), <https://www.scmp.com/news/china/politics/article/3247525/china-targets-devices-it-says-are-used-send-flight-data-foreign-entities#> [<https://perma.cc/9TJF-FLT9>].

110. Gabriella Godlewski, Note, *Private Jet Use by Celebrities Causes Climate Crisis to Soar to New Heights*, 11 JOULE: DUQ. ENERGY & ENV’T L.J. 5, 13 (2023).

111. Olga Gurtovaya, Comment, *Maintaining Privacy in a World of Technological Transparency? The BARR Program’s Ups and Downs in Changing Times*, 77 J. AIR L. & COM. 569, 587 (2012).

112. See Matt Burgess, *The Last Hour of Prigozhin’s Plane*, WIRED (Aug. 24, 2023, 12:22 PM), <https://www.wired.com/story/plane-crash-yevgeny-prigozhin-russia/> [<https://perma.cc/T22E-JFFT>] (“FlightRadar is one of a tiny number of sources of verifiable information about the fate of the Embraer Legacy 600 and, by extension, those onboard the plane.”); see also Ian Petchenik, *Flightradar24 Data Regarding the Crash of Ethiopian Airlines Flight 302*, FLIGHTRADAR24 (Mar. 4, 2021), <https://www.flightradar24.com/blog/flightradar24-data-regarding-the-crash-of-ethiopian-airlines-flight-302/> [<https://perma.cc/PP8G-A4KX>].

113. See Brenna Smith, *An FBI Surveillance Plane Has Been Circling West Baltimore*, BALTIMORE BANNER (June 1, 2023, 5:30 AM), <https://www.thebaltimorebanner.com/community/criminal-justice/fbi-spy-plane-baltimore-OKQGESMCSRDUDBOEOW6JH3EQ6A/> [<https://perma.cc/866G-SHRM>].

114. See Beth Warren, *How a ‘Narco-Plane’ Expert Headed Off a Major Cartel Drug Shipment into the US*, COURIER J. (June 30, 2023, 5:57 PM), <https://www.courier-journal.com/story/news/investigations/2023/06/28/mexican-drug-cartels-look-for-private-jets-near-orlando-to-ship-cocaine/70258020007/> [<https://perma.cc/8QWR-Q25K>] (“Suspicious flight patterns are flagged by HSI’s Air and Marine Operations Center in Riverside, California, which helps detect and track boats and planes and provide intelligence to agents . . .”).

115. See Scott Glasser, *Combating Illicit Activity by Tracking Flight Data via the Cloud*, AWS: PUB. SECTOR BLOG (Mar. 12, 2021), <https://aws.amazon.com/blogs/publicsector/combating-illicit->

*D. Carbon Offsets: A Path Out of the (Polluted) Woods?*¹¹⁶

A common refrain echoed by celebrities monitored by flight-tracking bots—and sometimes by their loyal fans¹¹⁷—is that, because they purchase carbon offsets,¹¹⁸ the public has no legitimate interest in their flight data, at least in terms of environmental impact.¹¹⁹ However, the reality behind carbon offsets is much more complicated than their proponents would like, and their effectiveness is still being evaluated—especially because “[t]hey are loosely regulated and investigations by news organizations in recent years have shown some programs overestimate how much carbon is being captured or have questionable practices.”¹²⁰

For example, The Guardian reported that “[t]he forest carbon offsets approved by the world’s leading certifier and used by Disney, Shell, Gucci and other big corporations are largely worthless and could make global heating worse”¹²¹ According to the reporters’ investigation “into Verra, the world’s leading carbon standard[,] . . . more than 90% of their rainforest offset credits—among the most commonly used by companies—are likely to be ‘phantom credits’ and do not represent genuine carbon reductions.”¹²² Another report on “almost 300 carbon offset projects” found that more of “the industry’s top registries have consistently allowed developers to claim

activity-tracking-flight-data-cloud/ [https://perma.cc/DM8P-W958]; see also Angela Wang, *The FAA Accidentally Disclosed More than 2,000 Flight Records Associated with Jeffrey Epstein’s Private Jets*, BUS. INSIDER (Nov. 29, 2021, 12:05 PM), <https://www.businessinsider.com/faa-accidentally-released-jeffrey-epsteins-flight-records-2021-10> [https://perma.cc/4HCM-UZ8L].

116. “[L]ike we stood a chance[, t]wo paper airplanes flying, flying, flying. And I remember thinking . . . Are we out of the woods? Are we in the clear yet?” TAYLOR SWIFT, *Out of the Woods (Taylor’s Version)*, on 1989 (TAYLOR’S VERSION) (Republic Records 2023).

117. See Louise Boyle, *Even Taylor Swift’s Biggest Fans Are Struggling to Defend Her Private Jet Use*, THE INDEP. (Feb. 12, 2024, 4:27 PM), <https://www.independent.co.uk/climate-change/news/taylor-swift-private-jet-super-bowl-b2494881.html> [https://perma.cc/4YT2-BF82].

118. Carbon offsets are “tradable ‘rights’ or certificates linked to activities that lower the amount of carbon dioxide (CO₂) in the atmosphere.” Angelo Gurgel, *Carbon Offsets*, MIT CLIMATE PORTAL (Nov. 8, 2022), <https://climate.mit.edu/explainers/carbon-offsets> [https://perma.cc/4T7R-Z5WU]. “By buying these certificates, a person or group can fund projects that fight climate change, instead of taking actions to lower their own carbon emissions. In this way, the certificates ‘offset’ the buyer’s CO₂ emissions with an equal amount of CO₂ reductions somewhere else.” *Id.*

119. See Harwell, *supra* note 8; see also Isabella O’Malley, *Why Taylor Swift’s Globe-Trotting in Private Jets Is Getting Scrutinized*, AP NEWS (Feb. 2, 2024, 10:18 PM), <https://apnews.com/article/taylor-swift-climate-jet-carbon-emissions-kelce-chiefs-02ac425d24281bd26d73bfd4590bc82> [https://perma.cc/V7SE-EZGP] (“[Bill] Gates has defended his travel by private plane by saying he purchases offsets and supports clean technology and other sustainability initiatives.”).

120. O’Malley, *supra* note 119.

121. Patrick Greenfield, *Revealed: More than 90% of Rainforest Carbon Offsets by Biggest Certifier Are Worthless, Analysis Shows*, THE GUARDIAN (Jan. 18, 2023, 9:00 AM), <https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe> [https://perma.cc/7YXL-DJ7E].

122. *Id.*

far more climate-saving benefits than justified.”¹²³ Therefore, celebrities should not take too much comfort in relying on carbon offsets to mitigate the effects of their emissions nor to mollify the concerns of climate activists.

E. Challenges to Tightening Requirements for Data Suppression Posed by the Government Speech Doctrine and Agency Capture

Given the legitimate public interest in private flight data and the little oversight the general public has into administrative decisions made to restrict the dissemination of flight information, Section 566,¹²⁴ the statutory basis for the LADD program for years, was surprisingly permissive to private flyers, mandating that the FAA block registration numbers merely “upon request” from private owners and operators—without requiring that requesters demonstrate any particular reason for their requests in exchange.¹²⁵ While Section 44114(c) will require that requesters attest to a safety or security need to apply for new ICAO aircraft identification codes, the provision is silent on what constitutes a safety or security need warranting a new code.¹²⁶ Additionally, Sections 44114(a) and (b) require the FAA to withhold aircraft registration numbers, other similar identifiable data or information, and certain types of personally identifiable information merely “upon [the] request of . . . private aircraft owner[s] or operator[s].”¹²⁷

Further, efforts to impose new requirements upon requesters—at least for Sections 44114(a) and (b)—outside of further amending Section 44114’s language could not only raise concerns of compelled speech among private operators¹²⁸ but would also likely be rendered futile due to the government speech doctrine. “According to the Supreme Court’s government speech doctrine, once speech is deemed government speech, it falls outside the

123. Natasha White, *Bogus Carbon Credits Are a ‘Pervasive’ Problem, Scientists Warn*, TIME (Mar. 21, 2023, 9:42 AM), <https://time.com/6264772/study-most-carbon-credits-are-bogus/> [<https://perma.cc/RG2Q-WLZL>].

124. 49 U.S.C. § 44103 note (Right to Privacy When Using Air Traffic Control System), *repealed* by FAA Reauthorization Act of 2024, Pub. L. No. 118-63, § 803, provided in relevant part:

Notwithstanding any other provision of law, the Administrator [of the Federal Aviation Administration] shall, upon request of a private aircraft owner or operator, block the registration number of the aircraft of the owner or operator from any public dissemination or display, except in data made available to a Government agency, for the noncommercial flights of the owner or operator.

125. *See id.*; *see also* *File a Request Aircraft Tail Number Blocking/Unblocking*, FAA, <https://www.faa.gov/pilots/ladd/request> [<https://perma.cc/MF42-DYTN>]; *infra* Section III.B.

126. *See* FAA Reauthorization Act of 2024 § 803.

127. *Id.*

128. However, those raising such concerns would face difficulty in the courts, as the current “compelled speech . . . cases . . . acknowledge that government-crafted messages will often be required as an incident of legitimate government programs.” Note, *The Curious Relationship Between the Compelled Speech and Government Speech Doctrines*, 117 HARV. L. REV. 2411, 2422 (2004).

purview of the Free Speech Clause.”¹²⁹ Because the government through the FAA both mandates ADS-B equipage and manages associated data through its regulatory scheme and enforcement mechanisms, these decisions regarding its dissemination undoubtedly deserve some protection under the government speech doctrine—and the Supreme Court has recognized similar activity as protected government speech.¹³⁰ Additionally, the FAA faces limits to changes it can make within its own programs based on statutory authorizations and agency precedent¹³¹—and it has been accused of acting “arbitrarily and capriciously” in previous efforts to modify its regulations.¹³²

While the government through the FAA has a right to “speak” by controlling its own data, we should be concerned by what message it sends in selectively allowing private flyers to filter their data without meaningful restraint.¹³³ This practice, at best, is an oversight, and at worst, exemplifies agency capture—the “undue control and domination of federal administrative agencies, particularly by identifiable private parties that are subject to the regulatory authority of the agency.”¹³⁴ The negative impacts of such private interests are enhanced when a “relatively small group of government officials . . . is in some way insulated from the impact of normal political forces,” subjecting agency officials to “extensive pressure” seeking to advance the private interest “at the expense of some broader interest of the public as a whole.”¹³⁵ Although the current data suppression programs have not developed enough to close the loophole allowing for unfiltered

129. Caroline Mala Corbin, Essay, *Government Speech and First Amendment Capture*, 107 VA. L. REV. ONLINE 224, 225 (2021).

130. See *Walker v. Tex. Div., Sons of Confederate Veterans, Inc.*, 576 U.S. 200, 212 (2015) (holding government-managed specialty license plate designs serving “governmental purposes of vehicle registration and identification” were government speech and therefore denial of an application for a design with a Confederate flag did not violate a nonprofit organization’s First Amendment rights).

131. “[W]e insist that an agency ‘examine the relevant data and articulate a satisfactory explanation for its action.’ . . . An agency may not, for example, depart from a prior policy *sub silentio* or simply disregard rules that are still on the books.” *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 513–15 (2009) (quoting *Motor Vehicle Mfrs. Ass’n of the United States, Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983)); see also *Administrative Procedure Act*, 5 U.S.C. §§ 551–559.

132. See *Opening Brief for Petitioners at 15–34, Nat’l Bus. Aviation Ass’n v. FAA*, 2013 WL 5610241 (D.C. Cir. Aug. 29, 2011) (No. 11-1241).

133. For example, a message possibly indicating a motive to aid private flyers in their efforts to “protect the refined sensibilities of elites from the unwanted gaze of their social inferiors.” Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1304 (2010) (discussing some of the reasons driving Warren and Brandeis’s introduction of the right to privacy to American jurisprudence).

134. Mark C. Niles, *On the Hijacking of Agencies (and Airplanes): The Federal Aviation Administration, “Agency Capture,” and Airline Security*, 10 AM. U. J. GENDER SOC. POL’Y & L. 381, 390 (2002) (footnote omitted).

135. *Id.* at 387–88.

private flight tracking, experts anticipate that they soon will¹³⁶—especially in light of new directives from Section 44114—which would severely curtail the public’s already limited ability to police the more reprehensible behaviors of the uber-rich.

F. The ADS-B Receiver: A Hobbyist’s Accessory or a New Pandora’s Box?

In the past fifteen years, attitudes have changed drastically regarding the public’s entitlement to view live flight data. In 2011, before ADS-B flight tracking had become commonplace, the Obama Administration encountered dogged opposition when it announced planned restrictions to LADD’s predecessor, the Block Aircraft Registration Request (BARR) Program. The Obama Administration “plann[ed] to severely restrict access to the BARR program” by directing the FAA to “begin releasing after-the-fact flight data on jet travel . . . unless the plane’s owner [could] provide the agency with a ‘Certified Security Concern’ memo explaining why the aircraft’s flight patterns should be excluded from the public databases.”¹³⁷ However, after intense lobbying and a court challenge by the Aircraft Owners & Pilots Association (AOPA) and the National Business Aviation Association (NBAA), the FAA “dropped the BARR restrictions.”¹³⁸

In the midst of BARR’s administrative drama, many in the political and legal spheres condemned the restrictions as an attack on privacy¹³⁹—even an ACLU representative asserted that “no plane’s flight history should be released to the public.”¹⁴⁰ Today, crowdsourcing of data has opened a Pandora’s Box of “open-source intelligence,” where “nonstate actors and

136. Doug Gollan, *Teen Who Tracked Elon Musk’s Private Jet Stirs Security Response*, FORBES (Mar. 18, 2022 2:33 PM), <https://www.forbes.com/sites/douggollan/2022/02/02/elon-musk-private-jet-tracker-likely-to-stir-industry-response/?sh=170bbcfelc5f> [<https://perma.cc/ZN6N-WGP9>] (“David Hernandez, an aviation attorney . . . and former prosecutor at the FAA as well as a DOT Honors Attorney, predicts, ‘The loophole will be fixed.’”); see also Mark Phelps, *FAA Announces More Privacy for Aircraft Operators*, AVWEB (Feb. 8, 2024), <https://www.avweb.com/aviation-news/faa-announces-more-privacy-for-aircraft-operators/> [<https://perma.cc/SPD4-WEWG>] (discussing the FAA’s expansion of the PIA program to “include more offshore airspace and routes traversing the Gulf of Mexico”).

137. Corbin Hiar, *BARR Battle: Corporate Jet Privacy Threatened by Obama Administration*, HUFFPOST (Dec. 6, 2017), https://www.huffpost.com/entry/barr-battle-corporate-jet_b_900397 [<https://perma.cc/2QAB-KWES>].

138. Dan Namowitz, *BARR Program Reinstated*, AOPA (Dec. 28, 2011), <https://www.aopa.org/news-and-media/all-news/2011/december/28/barr-program-reinstated> [<https://perma.cc/GN8E-B8DR>].

139. See, e.g., Gurtovaya, *supra* note 111, at 603 (“Today the FAA may be taking away the privacy of executives and businesses, but tomorrow it may be your privacy.”); Hiar, *supra* note 137 (describing how several U.S. senators, including Jon Tester, Mark Warner, and Amy Klobuchar, “protest[ed] the planned restriction”).

140. Hiar, *supra* note 137.

individuals [routinely] collect and analyze intelligence . . . sometimes more easily, more quickly, and better than governments.”¹⁴¹

Crowdsourced ADS-B data is one of the more high-profile examples of open-source intelligence, and third parties’ creation of essentially a “mirror[]”¹⁴² of FAA data presents challenges the architects of NextGen likely could not have anticipated in their attempts to promote a safer airspace. While the FAA maintains some sway over third-party aggregators, any serious efforts to restrict their monitoring of ADS-B signals, such as through encryption¹⁴³ or regulation, will undoubtedly conjure in the minds of many an unflattering resemblance with certain authoritarian regimes.¹⁴⁴

III. PUBLIC INTERESTS DEMAND STRONGER PROTECTIONS FOR FLIGHT TRACKING BOTS

As decisionmakers navigate relatively uncharted territory in regulating both independent aggregators and FAA data suppression programs, the choices they make over the next decade could dramatically impact the free flow of information and the security of private flyers. This power inherent in flight data necessitates that they take care to balance the public’s right to know with legitimate privacy and safety interests. The following measures would help decisionmakers strike the right balance.

A. *Flight-Tracking Bots Should Be Protected Under the First Amendment*

Not only do flight-tracking bots act as “direct extensions of their human creators,” they also “promulgat[e] useful information for the rest of us.”¹⁴⁵ Moreover, “one of the key purposes of free speech is to further the interests

141. Amy Zegart, *Spies like Us: The Promise and Peril of Crowdsourced Intelligence*, 100 FOREIGN AFFS. 168, 168–69 (2021).

142. Nadira Goffe, *Can Taylor Swift Really Sue the College Student Tracking Her Private Jet?*, SLATE (Feb. 9, 2024, 12:58 PM), <https://slate.com/culture/2024/02/taylor-swift-private-jet-emissions-tracker-jack-sweeney-cease-and-desist.html> [<https://perma.cc/BM8G-BJAH>].

143. For some proposals on ADS-B signal encryption, see, for example, Jamal Habibi Markani, Abdessamad Amrhar, Jean-Marc Gagné & René Jr Landry, *Security Establishment in ADS-B by Format-Preserving Encryption and Blockchain Schemes*, APPLIED SCIS., Feb. 28, 2023, at 1; S.S. Shavrin, T.G. Lavrentyeva, O.Y. Musatova, N.E. Kalabekyanc & A.B. Semenov, *ADS-B Cybersecurity and Autonomy—A-network*, 2023 SYS. SIGNAL SYNCHRONIZATION, GENERATING AND PROCESSING TELECOMMS., July 17, 2023.

144. For example, China, see Ye & Lee, *supra* note 109, and Saudi Arabia, see Ling, *supra* note 108.

145. Matt Field, *Do Social Media Bots Have a Right to Free Speech?*, BULL. ATOMIC SCIENTISTS (Jan. 9, 2019), <https://thebulletin.org/2019/01/do-social-media-bots-have-a-right-to-free-speech/> [<https://perma.cc/6F8A-L3RJ>]; see also Lamo & Calo, *supra* note 102, at 1005–06 (“Even when a great degree of attenuation exists between the human creator and the final speech product, the First Amendment may still protect the communication, because it protects not only the right to speak but also the right to receive information.”).

of *listeners*.”¹⁴⁶ Just as “voters need information to decide for whom to vote,”¹⁴⁷ the general public needs information to discern which people and entities deserve their attention and disposable income—whether they practice what they preach environmentally,¹⁴⁸ whether they use air traffic resources and taxpayer money for legal activities,¹⁴⁹ and whether they associate with actors who uphold human rights.¹⁵⁰ Therefore, both the courts and regulators have a responsibility to protect the free expression of both owners against censorship from private interests.

B. The Statutory Basis for the FAA’s Flight Data Suppression Programs Should Be Interpreted Narrowly and Amended to Impose Additional Requirements on Requesters

Further, while Section 44114’s “safety or security need” attestation requirement for new ICAO aircraft identification codes is a step in the right direction, its new provisions restricting dissemination of registration numbers and other information merely upon request are inconsistent with the principles of the First Amendment. While “the First Amendment has ‘permitted restrictions upon the content of speech in a few limited areas,’”¹⁵¹ allowing private operators to silence maintainers of the system they benefit from to keep taxpayers who fund that system¹⁵² in the dark about their activities perverts those limited exceptions.

146. Sacharoff, *supra* note 21; *see also* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) (“It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail, rather than to countenance monopolization of that market, whether it be by the Government itself or a private licensee.”).

147. Sacharoff, *supra* note 21.

148. *See* Justin Worland, *Why You Should Care About Celebrities’ Climate Hypocrisy*, TIME (Aug. 30, 2022, 2:49 PM), <https://time.com/6209448/california-drought-celebrities-climate-hypocrisy/> [<https://perma.cc/CH6W-CMJQ>] (“If the primary role of celebrities when it comes to climate change is telling us how to feel, the message is clear: the public should feel that conspicuous consumption is desirable no matter the climate implications.”).

149. *See, e.g.*, Warren, *supra* note 114; Glasser, *supra* note 115; *see also* Tran Nguyen, *Texas Sheriff Recommends Criminal Charges for Martha’s Vineyard Migrant Flights*, NBC10 BOS. (June 6, 2023, 2:22 PM), <https://www.nbcboston.com/news/local/fltexas-sheriff-recommends-criminal-charges-for-marthas-vineyard-migrant-flights/3061136/> [<https://perma.cc/BGZ4-ETJW>].

150. *See* Reed Johnson & Rick Rojas, *Public Consequences of Pop Stars’ Private Gigs*, L.A. TIMES (Mar. 10, 2011, 7:12 PM), <https://www.latimes.com/entertainment/la-et-music-dictators-20110311-story.html> [<https://perma.cc/EY6S-87ZF>] (“Despite the potential ethical breaches, . . . big stars likely will continue to be tempted by fat fees and all-expense-paid trips by private jet to a remote tropical island or luxury resort.”).

151. *Counterman v. Colorado*, 600 U.S. 66, 73 (2023) (quoting *United States v. Stevens*, 559 U.S. 460, 468 (2010)). “Historic and traditional categories” of limitations include “incitement, . . . defamation, and ‘true threats’ of violence.” *Id.* at 73–74 (quoting *Virginia v. Black*, 538 U.S. 343, 359 (2003)).

152. *See* David Koenig, *Biden Proposes Tax Increase on Fuel for Private Jets, Casting It as Making Wealthy Pay Their Share*, AP NEWS (Mar. 11, 2024, 1:17 PM), <https://apnews.com>

The FAA should interpret Section 44114(c)'s ambiguous "safety or security need" requirement for new ICAO aircraft identification codes narrowly,¹⁵³ and stipulate that requesters demonstrate a basis for suppression of their flight information under judicially-recognized speech restrictions—such as upon the receipt of genuine threats of violence¹⁵⁴—as well as in certain circumstances to prevent unfair competition.¹⁵⁵ Further, Sections 44114(a) and (b) should be amended to similarly require the attestation of a safety or security need to restrict dissemination of registration information. While the initial front-end review would become more intensive, such a system would likely improve these programs' effectiveness by reducing the amount of data for the FAA to manage—especially in view of the programs' ongoing struggles.¹⁵⁶ Moreover, this would allow the FAA to devote more attention to protecting innocent recipients of credible threats, rather than those seeking to use its resources simply to avoid public scrutiny.¹⁵⁷ Additionally, devising a more open process could build trust with third-party aggregators, incentivizing them to use FAA data and comply with associated restrictions—and could potentially reduce pushback if the FAA

.com/article/fuel-tax-business-jets-biden-budget-aefab96e0479ac174d624374f30a5870 [https://perma.cc/B6M3-S68S] ("FAA's management of the national airspace . . . is mostly paid by airline passengers. . . . The administration says that private jets account for 7% of all flights handled by the FAA but less than 1% of taxes that fund the federal trust fund for aviation and airports.").

153. *Cf.* *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009) ("The . . . canon of constitutional avoidance . . . counsel[s] that ambiguous statutory language [should] be construed to avoid serious constitutional doubts."); *Loper Bright Enters. v. Raimondo*, 144 S. Ct. 2244 (2024) ("[R]esolution of statutory ambiguities involves legal interpretation Courts interpret statutes, no matter the context, based on the traditional tools of statutory construction, not individual policy preferences.").

154. In its attempts to limit the BARR Program during the Obama Administration, the FAA articulated a similar policy, which provided in relevant part:

[This] change to FAA policy and the MOA will disclose the aircraft on the ASDI (time-delayed) Web site unless the general aviation owner or operator, or on-demand aircraft, submits to the FAA a Certified Security Concern. A Certified Security Concern would be based on either (a) the facts and circumstances establishing a Valid Security Concern (i.e., a verifiable threat to person, property or company, including a threat of death, kidnapping or serious bodily harm against an individual, a recent history of violent terrorist activity in the geographic area in which the transportation is provided, or a threat against a company); or (b) the general aviation aircraft owner or operator satisfying the requirement for a bona fide business-oriented security concern under Treasury Regulation 1.132-5(m), "Employer-provided transportation for security concerns," 26 CFR 1.132-5(m).

Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI), 76 Fed. Reg. 32258 (proposed June 3, 2011).

155. *See Gurtovaya, supra* note 111, at 595 ("Businesses also worry that flight data may provide competitive rivals with valuable information, thereby tipping them off and leading to 'corporate espionage.' This becomes an issue particularly when take-offs and landings tip off rivals to merger and acquisition talks." (footnote omitted)).

156. *See supra* Part I.

157. Under the FAA's old flight data suppression system, BARR, private flyers concealed a "ministry's tax-exempt jet [trips] to Maui and the Fiji Islands . . . [and] the use of state planes by [the] South Dakota governor . . . [for] Republican Party functions and his sons' high school basketball games," among many other questionable flights. Grabell & Jones, *supra* note 25.

seeks to impose new encryption mechanisms or regulations on ADS-B receivers.

C. Celebrities and Decisionmakers Should Target Stalking, Not Speech

Stalking is a pervasive, yet under-prosecuted¹⁵⁸ crime that inflicts both psychological and physical violence upon the famous and the unknown alike. None of the discussion in this Note is intended to discount the very real pain that stalking victims endure while navigating a law enforcement system that is often less than sympathetic to their concerns, especially when it comes to cyberstalking and online harassment.¹⁵⁹ However, posting publicly-available information about public figures regarding activities about which there is a legitimate public interest is simply not stalking under existing statutes¹⁶⁰—and it has yet to be proven that any stalkers have successfully relied on aggregated flight data to victimize celebrity targets.¹⁶¹

If their chagrin toward flight tracking indeed stems from the very real threats imposed by serial stalkers, celebrities' anger is misplaced. Instead, they should look to the policies and laws that have allowed these stalkers to continue their threatening patterns of behavior—specifically, law enforcement practices that dismiss—and sometimes punish¹⁶²—victims,

158. See Leana A. Bouffard, Jeff A. Bouffard, Matt R. Nobles & LaQuana Askew, *Still in the Shadows: The Unresponsiveness of Stalking Prosecution Rates to Increased Legislative Attention*, 73 J. CRIM. JUST., Mar. 3, 2021, at 1, 2. (“[C]hallenges can result in low prosecution and conviction[] rates, with offenders offered the opportunity to plead to lesser charges . . . or prosecutors dropping charges entirely.”).

159. See Citron, *supra* note 89, at 343–44. This disregard is further pronounced when women report these crimes, as some “[p]olice officers insist that cyber gender abuse is ‘no big deal.’” *Id.* at 343. Instead, “[l]aw enforcers engage in a game of jurisdictional hot potato, leading victims to run in circles. . . . Victims give up, having wasted countless hours of time. Victims get the message that law enforcement will not help them.” *Id.* at 343–44.

160. See *supra* Section II.B.

161. See Drew Harwell & Taylor Lorenz, *Musk Blamed a Twitter Account for an Alleged Stalker. Police See No Link.*, WASH. POST (Dec. 18, 2022, 8:19 PM), https://www.washingtonpost.com/technology/2022/12/18/details-of-musk-stalking-incident/?_pml=1 [<https://perma.cc/QVG7-CRJP>]; see also WAGNER, *supra* note 5, at 252 (“Musk was suggesting that the alleged stalker had only known the location of the car because of the private jet account. In reality, the gas station incident happened almost twenty-four hours after @ElonJet posted that Musk had landed in Los Angeles. Plus, the gas station itself was twenty-six miles from the airport.”). More recently, Just Stop Oil activists trespassed at an airport in the United Kingdom to spray paint Taylor Swift’s plane after learning it landed there. Ultimately, they failed to locate the aircraft and instead vandalized two other jets at random. David Mouriquand, *Just Stop Oil Targets Taylor Swift’s Jet—and Fails to Locate It*, EURONEWS (June 20, 2024, 10:03 AM), <https://www.euronews.com/culture/2024/06/20/just-stop-oil-targets-taylor-swifts-jet-and-fails-to-locate-it> [<https://perma.cc/U3QL-KUZ5>].

162. In one case, after being stalked, kidnapped, and sexually assaulted, a victim was further defamed by investigators, who “accused . . . [her and her partner] of fabricating a kidnapping.” Evan Sernoffsky, *Vallejo to Pay \$2.5 Million to ‘Humiliated Couple’ Accused of Hoax in Real Kidnapping*, S.F. CHRON. (Mar. 16, 2018, 4:26 PM), <https://www.sfchronicle.com/news/article/Vallejo-kidnap-victim-and-fiancee-accused-of-hoax-12757846.php> [<https://perma.cc/5K7N-EFMF>]; see also Huskins v. City of Vallejo, No. 2:16-cv-00603, 2017 WL 2868534 (E.D. Cal. July 5, 2017).

and reforms that have myopically rendered stalking ineligible for bail or pretrial detention in the jurisdictions celebrities frequent.¹⁶³ Further, bad actors¹⁶⁴ who target aircraft or airport infrastructure should be prosecuted to the fullest extent of the law.¹⁶⁵

CONCLUSION

Over the past twenty years, ADS-B transponders have dramatically improved the efficiency and safety of aircraft and the passengers they carry—and, through the efforts of FAA data maintainers and hobbyists alike, have also provided the public with unprecedented visibility into the live movements of air traffic all around the world. However, ADS-B's tracking capabilities have also ushered in novel questions to reckon with, including whether passengers have a reasonable expectation of privacy in their flight data, whether there is a legitimate public interest in public figures' live flight information, and whether administrative agencies can and should regulate open-source intelligence maintained by third parties. As decisionmakers grapple with the far-reaching effects their policies will have on informational freedom and passenger security, they must work diligently to balance the public's right to know with privacy and safety interests by protecting the speech of flight-tracking bots; restricting suppression of flight information to instances of legitimate security risks and anticompetitive behavior; and penalizing stalkers, not speakers. Only by recognizing these interests and acting swiftly to address them may we quell the potential negative impacts of the "plane-arazzi" and those who aim to censor them.

*Savannah C. Olmstead**

163. See Gutenplan, *supra* note 17, at 228; see also McNicholas, *supra* note 17.

164. For example, some members of the British environmental activist group Just Stop Oil. See Mouriquand, *supra* note 161.

165. In the United States, federal prosecutors have multiple statutes in their arsenal to deter interference with aircraft and airport infrastructure. See, e.g., 18 U.S.C. § 32 (destruction of aircraft or aircraft facilities, a felony punishable by up to twenty years imprisonment); 49 U.S.C. § 46314 (entering aircraft or airport area in violation of security requirements, a felony punishable by up to ten years imprisonment).

* J.D. Candidate (2025), Washington University School of Law; M.B.A. (2021) and B.S.E.E. (2020), The University of Alabama. Thank you to Emma Kenny-Pessia, Haley Bills, Elizabeth Potterf, Kyle Lorey, Kaitlyn Salyer, Shawn Podowski, Alyssa Dantoin, and all of the other incredible members of the Volume 102 staff for their creativity and hard work reviewing this Note. I would also like to thank Professor Neil Richards and the creators of the show "Air Disasters," who inspired my choice of this topic. Finally, I would like to express my love and deepest gratitude to my family, significant other, and friends, who have supported me in all of my endeavors and provided honest and thoughtful feedback for even the smallest of projects. Any opinions or mistakes present in this Note are my own.