Fordham Urban Law Journal

Volume 44, *Number* 3 2017 *Article* 6

DRONE CITY

Drone Surveillance: The FAA's Obligation to Respond to the Privacy Risks

Jeramie D. Scott*

*

DRONE SURVEILLANCE: THE FAA'S OBLIGATION TO RESPOND TO THE PRIVACY RISKS

Jeramie D. Scott[*]

Introduction 767
I. FAA Modernization Act 769
A. The FAA and the Petition for a Drone Privacy Rulemaking.....771
B. The FAA, Drones, and Privacy.....772
C. EPIC v. FAA 775
II. Privacy Issues.....776
III. Lack of Legal Protections.....778
A. Fourth Amendment Law, Drones, and Aerial Surveillance.....780
B. The Third Party Doctrine and Drone Surveillance.....782
IV. Potential Market for Drone Data Collection.....785
V. Importance of Privacy in Public 787
VI. Why the FAA Should Regulate Drones.....789
A. Privacy Must be Addressed to Safely Integrate Drones into the National Airspace.....789
B. The FAA Modernization Act Requires the FAA to Address Privacy Issues 790
Conclusion.....792

INTRODUCTION

Imagine a scenario not too far off in the future where drones in the sky are a regular occurrence over densely populated urban areas. These drones do not need to be in the line of sight of an operator and do not need to be actively operated at all as they fly around autonomously. Some of the drones you can see but more are present

---

[*] EPIC National Security Counsel and Director of EPIC's Domestic Surveillance Project.

then the eye can discern. Some are flying too high to see and are too quiet to hear.

The drones constantly flying overhead are delivering packages, transporting people, monitoring traffic, checking infrastructure, providing building security, and monitoring the environment. You know that the drones carry all sorts of high-tech equipment. But you do not know exactly what technology is on the drone, what the surveillance capabilities are, what information these drones could be collecting about you and anyone else who happens to be in a public space, or how this information could be used or to whom the information could be disclosed. Going into public essentially means giving up your privacy in a way never imagined before with little to no say in the matter. To maintain any semblance of privacy in public requires extraordinary efforts that limit your ability to participate in modern society. You do not carry your smartphone or any other mobile device that connects to the internet,[1] you wear a hood and special tinted glasses to thwart ear,[2] iris,[3] and facial recognition,[4] and you randomize your gait.[5] You also wear gloves to prevent the capture of your fingerprints,[6] avoid driving your own car,[7] and avoid

---

1. Mobile devices periodically emit a wireless signal, referred to as a probe, to find wireless networks to connect to and these probes includes a unique number called a media access control ("MAC") address, which can be used to track your movements. Latanya Sweeney, *My Phone at Your Service*, FED. TRADE COMM'N (Feb. 12, 2014, 4:15 PM), https://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service [https://perma.cc/D5AK-H9SP].

2. Your ear may someday unlock your phone just like your finger. *See* Teo Armus, *Use Your Ear to Unlock Your Phone*, PSFK (June 30, 2015), https://www.psfk.com/2015/06/amazon-fire-ear-recognition-technology-amazon-patent.html [https://perma.cc/XH5X-E2HV].

3. The distance at which iris recognition can be performed is increasing. *See* Robinson Meyer, *Long-Range Iris Scanning Is Here*, ATLANTIC (May 13, 2015), https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/ [https://perma.cc/CGK3-MJ6R].

4. Facial recognition thwarting glasses are already a thing. Alex Perala, *New Glasses Can Thwart Facial Recognition*, FIND BIOMETRICS (Aug. 10, 2015), http://findbiometrics.com/glasses-thwart-facial-recognition-8104/ [https://perma.cc/6VGA-WX9L].

5. Gait analysis is now used more frequently to identify individuals. *See* Jim Giles, *Cameras Know You by Your Walk*, NEW SCIENTIST (Sept. 19, 2012), https://www.newscientist.com/article/mg21528835-600-cameras-know-you-by-your-walk/ [https://perma.cc/U3HX-8LQG].

6. A digital fingerprint can now be lifted from a sufficiently high-resolution photo. *See* Andy Boxall, *Careful, Your Fun Peace Sign Selfie May Lead to Identity Theft*, DIGITAL TRENDS (Jan. 11, 2017, 3:58 AM), http://www.digitaltrends.com/mobile/peace-sign-selfie-fingerprint-identity-theft-news/ [https://perma.cc/M9Q9-K93L]; *see also* Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, GUARDIAN (last updated Feb. 21, 2017),

using the new self-driving/flying drone cars[8]—you stick to walking, biking, or mass public transportation.

The description above sounds a lot like the beginning of a dystopian novel, but it is the current track we are on as drones are being integrated into the National Airspace with no privacy protections for public space. In 2012, the Federal Aviation Administration ("FAA") was tasked by Congress with integrating drones into the National Airspace. Five years later, the agency is still working on domestic drone integration but refuses to address privacy as the agency works to establish safety rules for drones despite identifying privacy as an important issue to address as drones are integrated into the National Airspace.[9]

Part I of this Article discusses the FAA Modernization and Reform Act of 2012. The subsections of this Part will discuss some of the relevant details of the Act, the petition of the FAA to address drone privacy after the Act was passed, and the FAA's changing relationship with privacy. Part II highlights the privacy issues created by the integration of drones. Part III will look at the lack of legal protections for privacy in public, and Part IV will provide an example of how these lack of protections provide incentives for companies to amass data on individuals in public for financial gain. Part V will discuss why privacy in public is so important, and Part VI will provide reasons why the FAA needs to address privacy as the agency integrates drones. Finally, the Article provides some concluding thoughts, including the most important action the FAA could force drone companies to do.

I. FAA MODERNIZATION ACT

On February 14, 2012, the FAA Modernization and Reform Act of 2012 ("FAA Modernization Act" or "the Act") was enacted, requiring the Federal Aviation Administration to establish drone regulations and implement drones into the National Airspace System ("National Airspace").[10] The Act established a number of

---

https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands [https://perma.cc/7UHP-J9D2].

7. *See* Kaveh Waddell, *Amazon Wants to Scan Your License Plate*, ATLANTIC (Oct. 12, 2016), https://www.theatlantic.com/technology/archive/2016/10/amazon-wants-to-scan-your-license-plate/503747/ [https://perma.cc/KV6L-6BY7].

8. *See generally Pop.Up: Urban Transport Reimagined*, AIRBUS, http://airbus-xo.com/pop-up-urban-transport-reimagined/ [https://perma.cc/5M5W-R3NU].

9. *See infra* Part I.

10. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11 (codified as amended at 49 U.S.C. (2012)).

requirements and deadlines for the FAA to meet. Section 332 of the Act requires the FAA to develop a "Comprehensive Plan" to integrate drones into the National Airspace.[11] The Comprehensive Plan was to be finished no later than 270 days after the FAA Modernization Act became law.[12] Congress set minimum requirements for the plan, including projections on the required public drone rulemaking with specific recommendations on "how the rulemaking will—"

> (i) define the acceptable standards for operation and certification of civil unmanned aircraft systems; (ii) ensure that any civil unmanned aircraft system includes a sense and avoid capability; and (iii) establish standards and requirements for the operator and pilot of a civil unmanned aircraft system, including standards and requirements for registration and licensing . . .[13]

The Comprehensive Plan was due to Congress within one year of the FAA Modernization Act becoming law.[14] At the same time Congress required the submission of the Comprehensive Plan, it also required the FAA to develop a five-year roadmap ("the Roadmap") for the introduction of drones into the National Airspace.[15]

The Act requires the FAA to implement the recommendations of the Comprehensive Plan through a public notice-and-comment rulemaking.[16] The notice for the Comprehensive Plan rulemaking was due within eighteen months after the Comprehensive Plan was due to Congress.[17] The final rule was then to be published within sixteen months after the notice of the Comprehensive Plan rulemaking.[18] Using all the deadlines set by Congress and adding up the months, the final rule was to be published within forty-six months of the enactment of the FAA Modernization Act, which would have been in December 2015.[19]

The FAA has completely failed to adhere to the timeline established by Congress. As of April 2017, over sixty months had passed since the enactment of the FAA Modernization Act, and not even the notice for the rulemaking to implement the Comprehensive

---

11. *Id.* § 332(a)(1).
12. *Id.*
13. *Id.* § 332(a)(2).
14. *Id.* § 332(a)(4).
15. *Id.* §§ 332(a)(4), 332(a)(5).
16. *Id.* § 332(b).
17. *Id.*
18. *Id.* § 332(b)(2).
19. *See id.* §§ 332(a)(4), 332(b).

Plan has been published. The Comprehensive Plan itself has been published but even that was delivered to Congress nearly nine months later than required.[20]

A. The FAA and the Petition for a Drone Privacy Rulemaking

Although the FAA has not yet conducted the rulemaking to implement the Comprehensive Plan as required by Congress, the agency has conducted one rulemaking on drone integration related to small commercial drones.[21] That small drone rulemaking seemingly highlighted a reversal by the agency to address privacy in a formal way as it worked to integrate drones into the National Airspace.[22] The notice for the rulemaking stated that privacy was "beyond the scope of this rulemaking" and concluded that the agency had no jurisdiction to regulate drone privacy.[23]

This statement and conclusion in the Notice of Proposed Rulemaking ("NPRM") for the small drone rulemaking seemingly went against the FAA's previous actions and words, as well as congressional intent. To understand why, this Article looks at the agency's history with privacy as it relates to drones.

As previously mentioned, the FAA Modernization Act became law in February 2012. Immediately after the enactment of the Act, the Electronic Privacy Information Center ("EPIC")[24] led a coalition of organizations, legal scholars, and technology experts to petition the FAA to establish drone privacy rules—noting that "[t]he increased use of drones poses an ongoing threat to every person residing within

---

20. *See* Letter from Anthony R. Foxx, U.S. Sec'y of Transp., to Hon. John D. Rockefeller IV, Chairman, Comm. on Com., Sci., & Transp., U.S. Senate, et al. (Nov. 6, 2013).

21. *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, et al.); FAA Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,064 (June 28, 2016) (to be codified at 14 C.F.R. pts. 21, 43, 61, et al.).

22. As explained later in this section, the FAA had indicated in its response to a drone privacy petition brought by EPIC that the agency would consider privacy in the small drone rulemaking but when the notice came out for the rulemaking, the FAA stated privacy was outside the scope.

23. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. at 9544, 9552.

24. The petition to the FAA was led by the Electronic Privacy Information Center ("EPIC"), a public interest research center based in Washington, DC that focuses public attention on emerging privacy and civil liberty issues. *See* EPIC, https://epic.org, https://perma.cc/L2S3-N4C8.

the United States."[25] Specifically, the petition called upon the FAA to conduct a separate rulemaking on the privacy issues raised by drones in the National Airspace.[26]

Nearly two and a half years after the EPIC-led coalition petitioned the FAA to conduct a drone privacy rulemaking, the agency responded.[27] In the FAA's response, the agency stated that "[a]fter reviewing [EPIC's petition], we have determined that the issue you have raised is not an immediate safety concern."[28] But, the agency also explained that "the FAA has begun a rulemaking addressing civil operation of small unmanned aircraft systems in the national airspace system. We will consider your comments and arguments as part of that project."[29] During that very project however, the FAA abruptly reversed the agency's prior response to the EPIC-led coalition petition for drone privacy rules, stating in the notice-of-proposed rulemaking for small drones that privacy was "beyond the scope of this rulemaking."[30] This decision was made all the more befuddling given the agency's prior work up to this point, including soliciting public comments on a privacy policy for the drone test sites required by the FAA Modernization Act.[31]

B. The FAA, Drones, and Privacy

After the FAA Modernization Act was passed in 2012, the FAA appeared to embrace privacy as the agency went through the process of integrating drones into the National Airspace. Within two months of the Act becoming law, Senator Edward J. Markey (D-MA) and Representative Joe Barton (R-TX) sent a letter to the FAA with several questions focused on privacy and the integration of drones

---

25. Letter from EPIC et al., to Michael P. Huerta, Fed. Aviation Acting Admin. (Feb. 24, 2012), https://epic.org/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf [https://perma.cc/FWZ7-2QNH].

26. *Id.* at 5.

27. Letter from Lirio Liu, Dir., Off. of Rulemaking, Fed. Aviation Admin., to Marc Rotenberg, Exec. Dir., EPIC (Nov. 26, 2014), https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf [https://perma.cc/A368-ETN7] [hereinafter Liu Letter].

28. *Id.* at 1.

29. *Id.*

30. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552 (proposed Feb. 23, 2015).

31. Unmanned Aircraft System Test Sites, 78 Fed. Reg. 12,259 (proposed Feb. 22, 2013).

into the National Airspace.[32] The legislators noted that although drones will have their benefits, they also "enable invasive and pervasive surveillance without adequate privacy protections."[33] The legislators wanted to know "how the FAA is addressing" the privacy implications of drones.[34] Markey and Barton noted that the rulemaking process required by the FAA Modernization Act afforded the agency the "opportunity and responsibility to ensure that privacy of individuals is protected and that the public is fully informed about who is using drones in the public airspace and why."[35]

In response to the letter, the FAA acknowledged the privacy risks associated with drones, stating, "[t]he FAA recognizes that there are privacy concerns related to UAS operations, and the agency will review these concerns in the context of the ongoing UAS rulemaking activities and integration plans."[36] Indeed, one of the early requirements of the FAA Modernization Act was the establishment of drone test sites, and the FAA not only proposed privacy provisions for the test sites, but also solicited feedback from the public on the provisions.[37]

The FAA's acknowledgement of the privacy risks raised by drones did not end with the agency's response to a letter from congressional members asking about drones and privacy, or soliciting comments on a privacy policy for drone test sites. The core documents required by the FAA Modernization Act, the Roadmap and the Comprehensive Plan, to guide the integration of drones into the National Airspace were very explicit about privacy being an important issue to address with drone integration.[38]

---

32. Letter from S. Markey & Rep. Barton, to Michael P. Huerta, Fed. Aviation Acting Admin. (Apr. 19, 2012), https://fas.org/irp/congress/2012_cr/drones041912.pdf [https://perma.cc/97AN-UFCQ].

33. *Id.*

34. *Id.*

35. *Id.*

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

37. Unmanned Aircraft System Test Sites, 78 Fed. Reg. 12,259 (proposed Feb. 22, 2013); *see also* Letter from Kathryn B. Thomson, Fed. Aviation Admin. Chief Counsel, to Marc Rotenberg, President, EPIC (Feb. 14, 2013).

38. *See generally* FED. AVIATION ADMIN., INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE NATIONAL AIRSPACE SYSTEM (NAS) ROADMAP (2013), https://www.faa.gov/uas/media/UAS_Roadmap_2013.pdf [https://perma.cc/PT2R-XUSU] [hereinafter ROADMAP]; JOINT PLAN. & DEV. OFF., UNMANNED AIRCRAFT SYSTEMS (UAS) COMPREHENSIVE PLAN (Sept. 2013), https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf [https://perma.cc/MP92-WTEZ] [hereinafter COMPREHENSIVE PLAN].

The FAA Modernization Act required the creation of "a 5-year Roadmap for the introduction of civil unmanned aircraft systems into the national airspace system."[39] The Roadmap includes a section entitled "Privacy and Civil Liberties Considerations."[40] In this section, the FAA recognizes that the potential increase in drones in the National Airspace "raises questions as to how to accomplish UAS integration in a manner that is consistent with privacy and civil liberties considerations."[41] The Roadmap does state that the "FAA's mission does not include developing or enforcing policies pertaining to privacy or civil liberties."[42] However, this statement does not preclude the agency from addressing privacy, and Congress also gave the FAA wide latitude and a mandate to address the issues associated with integrating drones and only insisted on minimum requirements for the scope of the Comprehensive Plan.[43]

The Act required a comprehensive plan that would make recommendations as to what issues needed to be addressed as part of integrating drones into the National Airspace, and was explicit that the recommendations of the Comprehensive Plan be implemented through public rulemaking.[44] The FAA's Comprehensive Plan was equally explicit in the need to address privacy, stating that "[m]embers of the NextGen SPC agree on the need to address privacy concerns of the public at large while safely integrating UAS in the NAS."[45] The Next Generation Air Transportation Senior Policy Committee ("Nextgen SPC") is chaired by the Secretary of Transportation and includes as it members the following individuals or their designee: the Administrator of the FAA, the Administrator of NASA, the Secretary of Defense, the Secretary of Homeland Security, the Secretary of Commerce, and the Director of the Office of Science and Technology Policy.[46] Despite the many statements by the FAA regarding the importance of addressing the privacy implications of drones, when it came time to actually address privacy in the small drone rulemaking, the FAA shied away from the subject.

---

39. Pub. L. 112-95, 126 Stat. 11 § 332(b)(5) (2012).

40. ROADMAP, *supra* note 38.

41. *Id.*

42. *Id.*

43. Pub. L. 112-95, 126 Stat. 11 § 332(a)(1).

44. *Id.* at §§ 332(a)-(b).

45. COMPREHENSIVE PLAN, *supra* note 38, at 7.

46. The Vision 100—Century of Aviation Reauthorization Act, Pub. L. No. 108-176, § 710(b), 117 Stat. 2490, 2584 (2003).

C. EPIC v. FAA

Although not the focus of this Article, to give a more complete view of the FAA and drone privacy, it is worth briefly describing the challenges brought by EPIC—a public interest organization focused on emerging privacy issues—against the FAA for the agency's failure to address the privacy risks raised by drones.

When the FAA denied EPIC's petition for a separate public rulemaking on drone privacy issues, the agency pointed to the upcoming small drone rulemaking as the appropriate opportunity for EPIC, other organizations, and the public to comment on concerns with privacy.[47] As discussed earlier, when it came time for the FAA to issue the notice-of-proposed rulemaking, the agency reversed course and stated that privacy was outside the scope of the rulemaking.[48]

In response to the reversal by the FAA to consider privacy in the small drone rulemaking, EPIC filed a petition for review with the D.C. Circuit. EPIC brought two challenges: 1) for the agency's denial of EPIC's petition; and 2) for the agency's failure to consider privacy in the context of the small drone rulemaking.[49] The D.C. Circuit ruled that with respect to the first challenge, EPIC was time-barred.[50] Concerning the second challenge, the Court ruled that the challenge was premature because the small drone rulemaking was not a final reviewable order.[51] The final rule for the small drone rulemaking was published in June 2016 and since then EPIC has filed another petition for review in the D.C. Circuit, which includes a challenge to the final rule.[52] As of April 2017, the case is still pending before the D.C. Circuit. As the integration of drones continues and drone technology rapidly advances, whether the FAA is forced to

---

47. Liu Letter, *supra* note 27.

48. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552 (proposed Feb. 23, 2015).

49. EPIC v. FAA, 821 F.3d 39 (D.C. Cir. 2016).

50. *Id.* at 41. EPIC was time-barred because the organization did not file a petition to review within the sixty days required by the Administrative Procedure Act. Additionally, the Court did not agree with EPIC that FAA's response was an ambiguous denial at best given the fact the agency stated it would consider privacy in an upcoming rulemaking.

51. *Id.* Under the Administrative Procedure Act, only a final action can typically be challenged and a notice of a proposed rule is not typically considered a final action and was not in this case despite the arguments of EPIC that the notice represented the final response (i.e. the denial) to EPIC's petition when the agency stated in the notice that privacy was outside the scope of the rulemaking.

52. Petition for Review, EPIC v. FAA, 821 F.3d 39 (D.C. Cir. 2016) (No. 16-1297).

address privacy concerns may have long-lasting implications for our privacy in public space.

II. PRIVACY ISSUES

Drones can carry sophisticated surveillance equipment, and "by virtue of their design, their size, and how [high] they can fly, [drones] can operate undetected in urban and rural environments."[53] The Defense Advanced Research Project Agency ("DARPA") created the Autonomous Real-time Ground Ubiquitous Surveillance-Infrared ("ARGUS-IR") system, which enables "a persistent, real-time, high-resolution, wide-area, day-night video survelliance capability"[54] The field of view is roughly sixty-five square miles and ARGUS-IR can track sixty-five objects within that field of view at the same time.[55] The U.S. Army mounted the ARGUS-IR on a drone capable of hovering for over twenty hours at an altitude in excess of 15,000 feet.[56] Drones in general are a flexible platform for various surveillance technologies and can be equipped with long-range zoom lenses, thermal imaging, night vision, radar, facial recognition and other biometric recognition capabilities, automated-license plate readers, and other sensors to gather personal information.[57]

What does all the technology available to drones mean for privacy? Simply put, it means drones pose a unique threat to privacy in public. Drones greatly increase the capacity for domestic surveillance because drones provide a cheap aerial surveillance platform to which numerous surveillance technologies can be attached. Although aerial

---

53. Jennifer Lynch, *Are Drones Watching You*, ELEC. FRONTIER FOUND. (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you [https://perma.cc/F6CB-7BM8].

54. DARPA, DEP'T OF DEF. FISCAL YEAR (FY) 2014 PRESIDENT'S BUDGET SUBMISSION, Exhibit R-2A, 13 (2013), http://www.darpa.mil/attachments/(2G3)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2014%20(Approved).pdf [https://perma.cc/3D2F-BYBH].

55. *US Army Unveils 1.8 Gigapixel Camera Helicopter Drone*, BBC NEWS (Mar. 8, 2012), http://www.bbc.com/news/technology-16358851 [https://perma.cc/4B7D-AVCE].

56. *See* David Hambling, *Special Forces' Gigapixel Flying Spy Eyes All*, WIRED (Feb. 12, 2009), https://www.wired.com/2009/02/gigapixel-flyin/ [https://perma.cc/ML9R-LKL5].

57. Ciara Bracken-Roche et al., *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada*, SURVEILLANCE STUD. CTR. 18-19 (Apr. 30, 2014), http://www.sscqueens.org/sites/default/files/Surveillance_Drones_Report.pdf [https://perma.cc/8QBC-3UVQ].

surveillance has been possible for some time, drones will alter both the economics and industry of aerial surveillance.[58]

Before drones, conducting aerial surveillance required the use of a helicopter or airplane. The expense of using either created three restrictions: 1) who could use airplanes or helicopters for aerial surveillance; 2) how often an airplane or helicopter could be used for aerial surveillance; and 3) for what purpose aerial surveillance would be used.[59] The economic limitations meant very few people had access to aerial surveillance, aerial surveillance was not used frequently, and the purposes for which aerial surveillance were used were narrow because the surveillance had to be worth the expense.[60] Under these circumstances, mass aerial surveillance was not practical.

Drones, however, have changed the economics of aerial surveillance, making it accessible to practically anyone. This change in economics also expanded the industry for aerial surveillance.[61] Drones are being built specifically for aerial surveillance to conduct environmental monitoring, infrastructure inspection, and agricultural workflow among many other applications.[62] The increased industry around drones means drone technology advances at an accelerated rate. Drones will eventually fly autonomously and carry increasingly sophisticated equipment.[63] And as drones get safer, more will fly

---

58. I am using the term surveillance in a broad manner that does not require observation by a person but encompasses any collecting of data or information that can be uniquely connected to an individual.

59. *See* Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, CONG. RES. CTR. 16 (Apr. 3, 2013), https://fas.org/sgp/crs/natsec/R42701.pdf [https://perma.cc/4VEC-ZULB].

60. In practice this meant only the government generally had the ability to occasionally conduct aerial surveillance operations for targeted purposes (i.e., not mass, persistent aerial surveillance).

61. *The Economic Impact of Unmanned Aircraft Systems Integration in the United States*, AUVSI 2 (Mar. 2013), https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf [https://perma.cc/EZU6-KVHP] (estimating that the drone industry will generate more than eighty-two billion dollars in economic impact and account for over 100,000 jobs).

62. *Id.*

63. Boeing has a patent for an autonomous drone that can be recharged through a tether at a charging station. Benjamin Zhang, *Boeing Just Patented a Drone That Can Fly Forever*, BUS. INSIDER (June 5, 2015), http://www.businessinsider.com/boeing-patent-mid-air-rechargeable-drones-2015-6 [https://perma.cc/TCC8-FDN3]. Raytheon has a patent that, based on the purpose of the drone, will identify the important surveillance data for human review. Vlad Shvartsman, *Raytheon Patent Cherry-picks Relevant Data*, UAV PATENT BLOG (July 12, 2015), http://www.uavpatents.com/raytheon-patent-cherry-picks-relevant-data/ [https://perma.cc/7K8M-GEQN].

over densely packed urban areas when delivering packages and providing other services. The omnipresence of drones over urban areas is ripe for the creation of drone mass surveillance for the purpose of commercial data collection. This will undermine our privacy in public in ways that will have a fundamental impact on our interaction in public space and participation in society.

An abundance of information can be gathered about individuals in public if drones are allowed to freely collect personal information in public space. Drones will have a multitude of ways to identify individuals with the ability to add facial recognition, license plate readers, MAC address or Wi-Fi tracking, and other capabilities to identify and track people. Drones, with these capabilities onboard, will be able to track individuals' movements in public space and collect information about where an individual goes on a daily basis and who an individual interacts with. Information about what church you attend, what doctors you've seen recently, what protests you've participated in, and what stores or other businesses you have entered could all be collected by various drones flying around the city and aggregated in one large database.[64] Furthermore, all this information could be subjected to big data analysis by sophisticated algorithms in order to glean additional information from the data.[65] The surveillance of the public by commercial entities might be a by-product of drones flying around for other reasons (e.g., delivering packages) or might be done specifically for financial gain and to provide law enforcement access to a wealth of data on the people in a particular city.[66] Without any legal protections for privacy in public this is the reality we face.

III. LACK OF LEGAL PROTECTIONS

Privacy law in the United States is generally a siloed affair. There is no overarching law or laws that provide general privacy protections for individuals for potentially sensitive, personal information from

64. In 2016 a private citizen hired Persistent Surveillance Systems to fly a small plane over Baltimore, Maryland to collect and retain surveillance of the city. The plane was equipped with a wide-area, real-time surveillance system that covered around thirty square miles that was described as "Google Earth with TiVo capability." Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ [https://perma.cc/J68N-2EPF].

65. *See* Bracken-Roche, *supra* note 57, at 46 ("Mass data collection afforded through the persistent data capture capabilities of UAVs can . . . collect a wealth of 'ambient' information across a wide range of terrestrial environments, including the people, objects, and behaviours that are occurring within them.").

66. *See* Reel, *supra* note 64.

commercial actors. The laws that provide privacy protections are very specific, in isolated areas, evidenced by the names of the laws. For example, the Video Privacy Protection Act, Drivers Privacy Protection Act, Health Insurance Portability and Accountability Act, Right to Financial Privacy Act, and Children's Online Privacy and Protection Act.[67]

The Fourth Amendment protects individuals from unreasonable searches and seizures by government actors.[68] These protections from a government search remain in place even when the government is trying to perform the search by going through a commercial entity that has already performed the search if the commercial entity is acting as an agent of the government.[69] For example, if a warrant was required to perform mass, indiscriminate surveillance with a drone of a city block, the authorities could not avoid the warrant requirement by getting the exact same surveillance data from a company like Persistent Surveillance Systems that actually does perform mass, indiscriminate aerial surveillance on behalf of law enforcement.[70] Currently, police can freely perform surveillance on any scale in public space without obtaining a warrant, and thus would not need a warrant to get the same data from a commercial entity. Fourth Amendment protections largely fall away in the context of information freely exposed to the public.[71]

Not only does the Fourth Amendment not protect data exposed to the public, it does not protect data voluntarily given to a third party.[72] If, for example, you signed up with a company to have the drones flying above constantly track your location in order to send personalized ads or coupons based on where you happen to be at any given moment, that location information can be obtained by the police without a warrant from the company using drones to track your movement—even if the location data was deemed the type of information that required a search warrant to obtain. The ability of law enforcement to obtain information about individuals from companies that interact with those individuals further undermines what protections the Fourth Amendment does provide.

---

67. *See* Paul M. Schwartz & Daniel Solove, *Information Privacy Statutes and Regulations 2008-2009* vii-viii, https://www.informationprivacylaw.com/wp-content/uploads/2015/10/IPL-Statutes-TOC.pdf [https://perma.cc/57BP-XGBT].

68. U.S. CONST. amend. IV.

69. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

70. *See* Reel, supra note 64.

71. See *infra* Part IV for a detailed discussion.

72. This is referred to as the third-party doctrine. See *infra* Parts III-IV for a discussion of the third-party doctrine.

A. Fourth Amendment Law, Drones, and Aerial Surveillance

The current state of the law means there is little to no protection for privacy in public space. Consequently, drones flying in our National Airspace are free to collect any data that is readily available from a public vantage point. This is particularly true for private commercial entities to which the Fourth Amendment does not apply. Thus individuals do not have a reasonable expectation of privacy against commercial entities in the same way they do against the government.[73] The privacy implications are further heightened by how the courts have applied the reasonable expectation of privacy to public space and the third-party doctrine, which will allow law enforcement to access data collected by commercial drones without a warrant when the information is collected in public space or the information is voluntarily handed over.[74]

Under the Fourth Amendment, people are protected from unreasonable searches and seizures by a standard known as the "reasonable expectation of privacy." The reasonable expectation of privacy test was first articulated in Justice Harlan's concurrence in *Katz v. United States.*[75] In *Katz*, the government had placed an electronic listening device outside a public phone booth to listen to the defendant's phone conversation.[76] The government used the defendant's side of the conversation as evidence in the case over the objection of the defendant.[77] Katz argued that the phone booth was a constitutionally protected space under the Fourth Amendment; the government argued that the phone booth was not constitutionally protected.[78]

The Court rejected the parties' formulation of the issue that focused on whether the phone booth was a constitutionally protected area, famously stating "the Fourth Amendment protects people, not places."[79] The Court explained that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[80] Based on this formulation of the issue, the Court found that "[t]he Government's activities in electronically listening to and recording the petitioner's words

---

73. *See Jacobsen*, 466 U.S. at 113.
74. *See* Katz v. United States, 389 U.S. 347, 351 (1967).
75. *Katz,* 389 U.S. at 361-62 (Harlan, J., concurring).
76. *Id.* at 348.
77. *Id.*
78. *Id.* at 351.
79. *Id.*
80. *Id.*

violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[81] In other words, Katz had a reasonable expectation of privacy in his conversation in the phone booth. Having found that a search was conducted, the Court went on to analyze whether the search was permissible under the Constitution and found it was not.[82] The Court consequently reversed Katz's conviction.[83]

The majority opinion alluded to the "reasonable expectation of privacy" test, but it was in Justice Harlan's concurrence that the specific test was expressed. In his concurrence, Justice Harlan articulated his understanding of the rule used in *Katz* and prior decisions, stating "that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[84]

As articulated and applied, the reasonable expectation of privacy test does not generally extend to information that "a person knowingly exposes to the public."[85] This reasoning was reflected in two Supreme Court cases that addressed aerial surveillance.

The Court considered whether aerial surveillance was a violation of privacy and the Fourth Amendment in *California v. Ciraolo*[86] and *Florida v. Riley*.[87] In both cases, the Court found that law enforcement's observation from public airspace did not violate the Fourth Amendment.[88]

In *Ciraolo*, police, acting on an anonymous tip, flew over the defendant's house in a private plane and were able to identify marijuana growing in the yard.[89] Despite the officers viewing a fenced-in backyard, the Court reasoned that "officer's observations

---

81. *Id.* at 353 (emphasis added).
82. *Id.* at 354-59.
83. *Id.* at 359.
84. *Id.* at 361 (Harlan, J., concurring).
85. *Id.* at 351.
86. California v. Ciraolo, 476 U.S. 207 (1986).
87. Florida v. Riley, 488 U.S. 445 (1989).
88. Interestingly, both cases indicated that what the officers could see with their "naked eye" from public airspace was not a violation of the Fourth Amendment. The "naked eye" line could be used to distinguish aerial observation from a manned-vehicle verse a drone but currently such a challenge has not been made and police readily use drones without warrants where specific state laws have not restricted them from doing so.
89. *Ciraolo*, 476 U.S. at 209.

from a public vantage point where he has a right to be and which renders the activities clearly visible" do not violate the Fourth Amendment.[90]

Similarly, in *Riley* the police were acting on an anonymous tip and flew a helicopter over a mobile home that had greenhouses located near it.[91] The greenhouses generally obscured the contents inside except for some missing roofing panels.[92] Through these missing panels, the police were able to identify marijuana in the greenhouse.[93] The Court in *Riley*, like in *Ciraolo*, argued the police "were likewise free to inspect the yard form the vantage point of an aircraft flying in the navigable airspace . . . ."[94]

Thus information exposed to the public, even if only exposed from aerial vantage points, can freely be collected by law enforcement drones.[95] Even though one may have a subjective expectation of privacy in public space, particularly in the aggregation of the data exposed while in public and any information that can be derived from the analysis of that data, this subjective expectation of privacy is not one the courts have recognized as accepted by the public.[96]

B. The Third Party Doctrine and Drone Surveillance

The lack of privacy in public is exacerbated by the third-party doctrine, which gives no Fourth Amendment protection to information freely given to a third party. The origins of the third-party doctrine are found within *United States v. Miller*.[97] In that case, Miller claimed Fourth Amendment protections for his banking records that were accessed by the government without a judicial warrant.[98] The Court ruled that Miller had no Fourth Amendment interest in his bank records that were revealed and consequently conveyed to the government by a third party (i.e. the bank).[99] The

---

90. *Id.* at 213.
91. *Riley*, 488 U.S. at 448.
92. *Id.*
93. *Id.*
94. *Id.* at 450.
95. Also, law enforcement can just get the information directly from the drone companies without the need for a warrant. *See supra* notes 71-72 and accompanying text.
96. *See Katz*, 389 U.S. at 351. *But see* United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring) (suggesting that individuals may have a reasonable expectation of privacy in their public movements).
97. United States v. Miller, 425 U.S. 435 (1976).
98. *Id.* at 436.
99. *Id.* at 445.

third-party doctrine was largely solidified in *Smith v. Maryland.*[100] In *Smith*, the Court ruled that the defendant did not have a Fourth Amendment interest in the phone numbers he dialed that were consequently passed to the phone company and collected by the government, stating "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[101]

In 2012, the Court in *United States v. Jones* began to recognize the problems with the third-party doctrine in a digital age,[102] but the cases that established the doctrine still remain binding precedent. In *Jones*, the government installed a global positioning system ("GPS") tracking device on a vehicle used by Jones.[103] The GPS device was installed on the vehicle while it was on private property, the day after the warrant expired, and in Maryland instead of the District of Columbia, where the warrant authorized installation.[104] The government subsequently tracked the vehicle for twenty-eight days.[105] The Court reviewed the lower court's decision that the warrantless attachment of the GPS device and the subsequent tracking constituted a search, and thus violated the Fourth Amendment.[106] In the majority opinion by the Court, written by Justice Scalia, the Court did not analyze whether a search occurred using the reasonable expectation of privacy test, instead using the common-law trespassory test.[107] In the concurrence, Justice Sotomayor wrote "[w]hen the Government physically invades personal property to gather information, a search occurs."[108] With respect to collecting the same GPS data without a trespass, Justice Scalia suggested "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[109]

Although the majority opinion in *Jones* did not address whether GPS tracking for an extended period of time constitutes a search under the reasonable expectation of privacy test, a majority of Justices agreed that it did in the concurrences. Both Justice Alito and

---

100. Smith v. Maryland, 442 U.S. 735 (1979).
101. *Id.* at 745.
102. 565 U.S. 400 (2012).
103. *Id.* at 403.
104. *Id.*
105. *Id.*
106. *Id.* at 404 (citing United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010)).
107. *Id.* at 409.
108. *Id.* at 414 (Sotomayor, J., concurring).
109. *Id.* at 412.

Justice Sotomayor wrote concurrences supporting a reasonable expectation of privacy analysis that found that the GPS tracking constituted a search under the Fourth Amendment.[110] Justice Alito's concurrence was joined by Justices Ginsburg, Breyer, and Kagan.[111] Those four justices combined with Justice Sotomayor constitute what has been referred to as a "shadow majority."[112]

Both the Alito concurrence and Sotomayor concurrence show concern for the prospect of creating the same compilation of GPS data as in *Jones*, but without any physical intrusion.[113] Justice Sotomayor acknowledged the growing issue of the third-party doctrine in our digital society, stating:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[114]

Justice Sotomayor's position that the Court should reconsider the third-party doctrine is a step in the right direction, if only a partial one. Unfortunately, information freely exposed to the public that a drone can collect may need more protection than a new precedent that overturns the third-party doctrine. In the cases that established the third-party doctrine, the data in question was only given to a distinct and definable third party, leaving room to distinguish data collected strictly from public space since that data is, in some sense, freely exposed to the public.[115] On the other hand, many of the risks associated with GPS tracking highlighted by Justice Sotomayor in her concurrence are applicable to mass surveillance by drones of public space. For example, in *Jones*, Justice Sotomayor acknowledged the chilling effect to First Amendment associational and expressive

---

110. *Id.* at 413-18 (Sotomayor, J., concurring); *id.* at 418-19 (Alito, J., concurring).

111. *Id.* at 418 (Alito, J., concurring).

112. The "shadow majority" references the fact that the reasoning in the concurrences was not the basis of the majority opinion, but does suggest that the Court would have had enough judges to consider long-term GPS tracking a search under the reasonable expectation of privacy test. *See, e.g.,* Orin Kerr, *Courts grapple with the mosaic theory of the Fourth Amendment*, WASH. POST: VOLOKH CONSPIRACY (Apr. 28, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/04/28/courts-grapple-with-the-mosaic-theory-of-the-fourth-amendment [https://perma.cc/Y5P3-AC9V]

113. *Jones,* 565 U.S. at 413-18 (Sotomayor, J., concurring); *id.* at 418-19 (Alito, J., concurring).

114. *Id.* at 417 (Sotomayor, J., concurring).

115. *Id.* at 418.

freedoms.[116] A similar chilling effect occurs with drone surveillance. Drones typically carry their own GPS devices, and with surveillance payloads that might include multiple ways to identify an individual, drones have the capacity to conduct the kind of long term GPS tracking Justice Sotomayor suggested has a chilling effect on First Amendment rights.

IV. POTENTIAL MARKET FOR DRONE DATA COLLECTION

The general lack of privacy protections in public space and the third-party doctrine create the possibility of mass surveillance by the private sector that will be fully accessible by law enforcement without the requirement for a judicial warrant. Indeed, businesses may purposefully collect data for the benefit, in part, of law enforcement agencies. Drones will fly over populated urban areas with an array of sophisticated equipment that can and will be used to collect data about the surrounding environment, including the people in that environment.

Without some baseline rules or regulations, drones could greatly increase the commercial industry of selling law enforcement access to databases of information obtained through the mass surveillance of public space. This type of market has developed with the technology of Automated License Plate Readers ("ALPRs").[117] Companies have taken advantage of the lack of privacy protections in public space to aggregate massive databases on the public.

Many law enforcement agencies pay for access to data collected by the private sector. Vigilant Solutions and its subsidiary, Digital Recognition Network ("DRN") are two of the many providers of license plate data to law enforcement.[118] Vigilant Solutions only sells its data to law enforcement officers.[119] DRN sells its data to a variety of third parties, including banks, the auto repossession industry, college security, and private investigators.[120]

---

116. *Id.* at 416.

117. Steve Orr, *License Plate Data is Big Business*, USA TODAY (Nov. 2, 2014), http://www.usatoday.com/story/news/nation/2014/11/02/license-plate-data-is-big-business/18370791/ [https://perma.cc/RAK5-D25Z].

118. *Vigilant Solutions*, DIG. RECOGNITION NETWORK, http://drndata.com/company/vigilant-solutions/ [https://perma.cc/2R9J-6T4X]; DIG. RECOGNITION NETWORK, http://drndata.com/company/ [https://perma.cc/ZX4F-7YJV].

119. *See National Vehicle Location Service*, VIGILANT SOLUTIONS, http://vigilantsolutions.com/products/nvls [https://perma.cc/4T44-SFR2].

120. Shawn Musgrave, *A Vast Hidden Surveillance Network Runs Across America, Powered by the Repo Industry*, BETABOS. (Mar. 5, 2014), http://www.betaboston.com/news/2014/03/05/a-vast-hidden-surveillance-network-runs-across-america-powered-by-the-repo-industry/ [https://perma.cc/2FAX-RMGB];

DRN collects data from thousands of private citizens who volunteer to mount ALPR cameras on their cars.[121] When the ALPR cameras spot a stolen vehicle, DRN pays the private citizen $200-$400.[122] Vigilant Solutions' collection of license plate records from law enforcement also incorporates data from DRN.[123] Vigilant Solutions' ability to leverage DRN's commercial collection of license plate records has created a database of over five billion license plate hits.[124] Other large providers of license plate services include L3 Mobile-Vision and ELSAG.[125] ELSAG LPRs are used by over 5000 law enforcement agencies around the world.[126]

But even if you allow drone companies to collect information that is not readily exposed to the public, law enforcement may still have easy access to it without a warrant. This is the case with social media. Many law enforcement agencies pay for social media monitoring.[127] The social media monitoring companies often get direct access to all the social media from a particular social media site, even to those users who limit public access to their social media. The social media monitoring companies provide access to law enforcement to the data and tools to analyze it all and do so with no warrant from the police because of the third-party doctrine discussed above.

---

see also Shawn Musgrave, *Massive License Plate Location Database Just Like Instagram, Digital Recognition Network Insists*, BETABOS. (Mar. 5, 2014), http://www.betaboston.com/news/2014/03/05/massive-license-plate-location-database-just-like-instagram-digital-recognition-network-insists/ [https://perma.cc/9F43-T2UC].

121. Gil Aegerter, *License Plate Data Not Just For Cops: Private Companies Are Tracking Your Car*, NBC NEWS (Jul. 19, 2013, 4:44 AM), http://www.nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677 [https://perma.cc/N8PM-CX2F].

122. Elizabeth Kreft, *Surveillance For Hire: Would You Take Money to Record Fellow Drivers?*, BLAZE (Mar. 6, 2014, 8:02 AM), http://www.theblaze.com/news/2014/03/06/surveillance-for-hire-would-you-take-money-to-record-fellow-drivers/ [https://perma.cc/S5EE-6T5N].

123. DIG. RECOGNITION NETWORK, *supra* note 118.

124. VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/ [https://perma.cc/96C3-HXY4].

125. L3 MOBILE-VISION, http://www.mobile-vision.com/products/alertvu/ [https://perma.cc/TVL7-YGE4];
ELSAG, https://www.elsag.com [https://perma.cc/AB2X-FB36].

126. Kim Zetter, *Even The FBI Had Privacy Concerns On License Plate Readers*, WIRED (May 15, 2015, 8:00 AM), https://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers/ [https://perma.cc/5559-RCP4].

127. *Map: Social Media Monitoring by Police Department, Cities, and Counties*, BRENNAN CTR. FOR JUST. (Nov. 16, 2016), https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties [https://perma.cc/LDF8-3JY2].

Drones have the potential to make aggregation of commercial surveillance data of public space big business. Drones are, in one sense, merely aerial surveillance platforms that can be loaded with an array of surveillance equipment. There are numerous identifiers that can be used to track individuals in public, including license plate readers as well as facial recognition technology and technology that can collect the MAC addresses that each mobile phone can be uniquely identified by.[128] Without protections for privacy in public, our physical public space will mirror online surfing where numerous entities are looking to track information about you as long as you are in public space.

V. IMPORTANCE OF PRIVACY IN PUBLIC

The concept of "privacy in public" can seem like an oxymoron at first glance, but the concept is absolutely essential to a well-functioning democracy. Privacy in public allows for self-realization;[129] it supports freedom of thought[130] and associational rights;[131] and privacy in public prevents conformity of thought and the chilling of speech,[132] thus protecting the free market of ideas that is vital for proper democratic discourse.

Traditional theories of privacy have focused on "securing intimate and personal realms."[133] The focus was on actual threats to privacy.[134] Not until the rise of information technology and databases was there a perceived threat to privacy in public.[135] Privacy in public was traditionally protected by economic and technological limitations that made public information largely obscure.

In an age before information technology, it would have been extremely hard to collect, analyze, and retain large amounts of public information over a long period of time for just one person, let alone millions. Aggregating disparate public records and surveilling the public activities of one individual would take a great deal of

---

128. *See generally supra* notes 1-6.

129. Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 37 (1976) ("I shall myself argue that the right to privacy is fundamentally connected to personhood.").

130. *Id.* at 39.

131. *Id.* at 30.

132. *Id.* at 43.

133. *See* Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207 (1997).

134. *Id.*

135. *See* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 142 (2014).

resources. The practical obscurity of actions in public meant large scale surveillance of public space was a minimal concern at best. But we are increasingly losing this obscurity and drones threaten to abolish it and make indiscriminate mass surveillance in public space an everyday occurrence.

Joel Reidenberg has used obscurity as a starting to point to understand the loss of privacy in public. Reidenberg describes this loss of practical privacy in three stages: (1) obscurity, (2) accessibility, and (3) transparency.[136] The obscurity stage precedes mass deployment of information technologies and preserves privacy in public through the sheer difficulty and cost of traditional surveillance.[137] The accessibility stage implements the technology that makes personal information accessible to the public.[138] Consider the ubiquity of cameras—from closed-circuit television to cell phones in everyone's hands—that can take pictures and record video. The digitization of public records would be another example.[139] The transparency stage takes all this newly accessible information and makes it readily available through technologies like search engines, social media sites, or large databases of license plate data.[140]

Drones threaten to make our activities in public both more accessible and more transparent, as all the data from the drones ends up in large, searchable databases for commercial exploitation. Drones will not only make public activities accessible and transparent but if the information drones collect is used to create databases, the data will be analyzed by sophisticated algorithms that derive additional information value.[141]

In the age of domestic drones, obscurity and privacy in public need to be protected. Privacy in public is vital to our democracy. We must continue to allow practical obscurity in public space to protect our privacy. Where we allow our public spaces to become bastions of mass surveillance we will see a slow degradation of civic engagement

---

136. *Id.*

137. *Id.* at 148.

138. *Id.* at 148-49.

139. *See, e.g.*, Anna Forrester, *FBI Completes Digitization of Criminal, Civil Identity Records*, EXEC. GOV'T (Aug. 22, 2014), http://www.executivegov.com/2014/08/fbi-completes-digitization-of-criminal-civil-identity-records-penny-harker-comments/ [https://perma.cc/BCR5-7U75].

140. *See* Reidenberg, *supra* note 135, at 150.

141. *See* Bracken-Roche et al., *supra* note 57, at 46 ("Mass data collection afforded through the persistent data capture capabilities of UAVs can . . . collect a wealth of 'ambient' information across a wide range of terrestrial environments, including the people, objects, and behaviours that are occurring within them.").

in public space.[142] As drones are increasingly deployed in our National Airspace, become more sophisticated, and mass surveillance of public spaces increases, it will have a detrimental impact on our democracy.[143] It is imperative that drone privacy is addressed now by the FAA as the agency integrates drones into the National Airspace.

VI. WHY THE FAA SHOULD REGULATE DRONES

Drones pose a unique threat to privacy. The FAA has not only acknowledged this threat to privacy, but the agency has even suggested that addressing this threat is necessary to integrating drones into the National Airspace.[144] Yet, the agency has either claimed that addressing privacy is outside the scope of the agency's work because its mission focuses on safety[145] or that the FAA Modernization Act does not require the agency to address privacy.[146] Though the agency has acknowledged the possible relationship between safety and privacy,[147] it fails to recognize the extent to which addressing privacy is necessary to safely integrate drones.

A. Privacy Must be Addressed to Safely Integrate Drones into the National Airspace

Without adequate drone privacy rules, self-help methods for protecting privacy will create the very safety risks the FAA seeks to avoid. In the Notice of Proposed Rulemaking for small drones, the FAA identified two safety concerns. First was the risk of drone operation without "the ability to see manned aircraft in the air in time to prevent a mid-air collision between the [drone] and another aircraft."[148] Second was a "loss of positive control" over the operability of a drone "due to a failure of the control link between the aircraft and the operator's control station."[149] The FAA states that

---

142. We've already seen this online after the Edward Snowden revelations. *See generally* PEN AM. CTR., GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS 5, 8 (2016), www.pen.org/sites/default/files/globalchilling_2015.pdf [https://perma.cc/3L6E-J6GU].

143. Individual privacy is necessary to maintain a well-functioning democracy. *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013).

144. *See* COMPREHENSIVE PLAN, *supra* note 38, at 4.

145. FAA Operation and Certifications of Small Unmanned Aircraft Systems Final Rule, 81 Fed. Reg. 42,064, 42,191 (June 28, 2016) (to be codified at scattered sections of 14 C.F.R.).

146. *Id.*

147. *See id.*

148. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9548 (proposed Feb. 23, 2015).

149. *Id.* at 9549.

the loss of positive control "could pose a significant risk to persons, property, or other aircraft."[150]

In response to the privacy fears surrounding drone surveillance, commercial industry has responded with privacy protective measures for individuals that can lead to loss of positive control and subsequently pose a significant risk to persons and property. One of these solutions is known as geo-fencing. Geo-fencing designates a specific geographic area as restricted air space.[151] The drones that are programmed to respect geo-fenced areas can be forced to avoid these restricted areas or even forced to land if they enter a restricted area—removing positive control from the drone operator. Some individuals opt for a more direct self-help option when encountering drones on or near their property. The concerns over privacy have resulted in individuals shooting down drones with guns,[152] a self-help method that has obvious risks, especially in densely populated urban areas.

When individuals and drone manufactures are left with no option other than to defend their privacy interests, they will create technologies and react in ways that make operating drones less safe. The privacy, property, and security interests behind the development of geo-fencing and the shooting down of drones are just two examples of why it is unreasonable to separate drone privacy from safety, and why the FAA must address privacy prior to authorizing widespread drone deployment.

B. The FAA Modernization Act Requires the FAA to Address Privacy Issues

Congress required the FAA to develop a Comprehensive Plan with specific recommendations for a rulemaking to "define the acceptable standards of operation and certification" of drones and to "establish standards and requirements for the operator[s] and pilot[s]" of

---

150. *Id.*

151. *See What is Geofencing?*, AISC, https://www.aisc.aero/what-is-geofencing/ [https://perma.cc/73QT-NDJG].

152. *See, e.g.*, Cyrus Farivar, *Kentucky man shoots down drone hovering over his backyard*, ARS TECHNICA (July 29, 2015), https://arstechnica.com/tech-policy/2015/07/kentucky-man-shoots-down-drone-hovering-over-his-backyard/ [https://perma.cc/YCN8-YLKZ]; Cyrus Farivar, *Woman Shoots Drone: "It Hovered for a Second and I Blasted it to Smithereens.,"* ARS TECHNICA (Aug. 29, 2016), https://arstechnica.com/tech-policy/2016/08/65-year-old-woman-takes-out-drone-over-her-virginia-property-with-one-shot/ [https://perma.cc/VSG5-5E4X]; Eugene Volokh, *Man arrested for shooting down a neighbor's drone*, WASH. POST: VOLOKH CONSPIRACY (Oct. 2, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/10/02/man-arrested-for-shooting-down-a-neighbors-drone/ [https://perma.cc/R34A-GC6L].

drones, as well as to identify "the best methods to ensure safe operation" of drones in the National Airspace.[153] The recommendations of the Comprehensive Plan were to be implemented by a notice and comment rulemaking.

In the FAA's Comprehensive Plan, the agency made clear that privacy issues need to "be taken into consideration as [drones] are integrated into the NAS."[154] The agency acknowledged that "concerns" about how drone operations impact privacy will "grow stronger" as "demand for [drones] increases."[155] The FAA specifically identified the work on drone test site rules as a way to "inform future rulemaking activities and other policy decisions related to safety, *privacy*, and economic growth."[156] The agency proposed that the "lessons learned and best practices established at the test sites may be applied more generally to protect privacy in [drone] operations throughout the [National Airspace]."[157]

Congress was clear in its mandate to the FAA to conduct "a notice of proposed rulemaking to implement the recommendations of the [Comprehensive] plan."[158] The FAA identified privacy in the Comprehensive Plan as one of the issues necessary to address for drone integration[159] and consequently the Act required the FAA to address privacy in its rulemaking to implement the Comprehensive Plan.

Indeed, Congress expected the FAA to address privacy. In an Explanatory Statement that accompanied the 2014 Consolidated Appropriations Act, Congress required the FAA to conduct a drone privacy study, stating:

> Without adequate safeguards, expanded use of UAS and their integration into the national airspace raise a host of concerns with respect to the privacy of individuals. For this reason, the FAA is directed to conduct a study on the implications of UAS integration into national airspace on individual privacy.[160]

The report specifically required the FAA to study "how the FAA can address the impact of widespread use of UAS on individual

---

153. FAA Modernization and Reform Act of 2012, Pub. L. 112-95, 126 Stat. 11, § 332(a)(2) (codified as amended in scattered sections of 49 U.S.C.).

154. COMPREHENSIVE PLAN, *supra* note 38, at 4.

155. *Id.* at 5.

156. *Id.* at 15 (emphasis added).

157. *Id.* at 7.

158. FAA Modernization and Reform Act § 332(b)(2) (2012).

159. COMPREHENSIVE PLAN, *supra* note 38, at 7.

160. 160 Cong. Rec. H1186 (daily ed. Jan. 15, 2014).

privacy as it prepares to facilitate the integration of UAS into the national airspace."[161] The report was to be submitted to Congress within eighteen months of enactment of that appropriations bill and completed "well in advance of the FAA's schedule for developing final regulations on the integration of UAS into the national airspace."[162] Nearly forty months later the report still has not been submitted to Congress. The FAA continues to avoid addressing privacy as Congress required the agency to do.

CONCLUSION

The FAA is the administrative agency with the statutory authority to issue drone operation licenses and maintain order in the National Airspace.[163] It is the most appropriate agency to oversee comprehensive privacy rules and regulations for drone operators. The FAA is uniquely positioned to ensure that transparency, accountability, and other privacy-protective principles of data collection are built in to the drone authorization process.

The integration of drones represents a pivotal moment to address the privacy implications of new technology prior to that technology saturating society. There are many things the FAA could do to mitigate the privacy risks posed by drones. Perhaps the most important thing the agency could do is demand public transparency: transparency in the surveillance technology and its capabilities that drones will carry, transparency in any collection, use, retention, or distribution of sensitive or personal information, and transparency of any algorithmic analysis of the information that seeks to glean personal or sensitive information from more innocuous data that has been collected.

Drones represent a unique threat to our public spaces that has received much publicity, and if we fail to proactively set baseline privacy safeguards for drones, we have little chance of addressing the privacy implications of other technologies that threaten to undermine our privacy.

---

161. *Id.*
162. *Id.* at H1187.
163. *See* FAA Modernization and Reform Act §§ 332-334.