Drones and Data: A Limited Impact on Privacy

David Sella-Villa

Follow this and additional works at: https://scholarship.richmond.edu/lawreview

Part of the Courts Commons, Judges Commons, Privacy Law Commons, State and Local Government Law Commons, and the Supreme Court of the United States Commons

Recommended Citation

Available at: https://scholarship.richmond.edu/lawreview/vol55/iss3/8

This Article is brought to you for free and open access by the Law School Journals at UR Scholarship Repository. It has been accepted for inclusion in University of Richmond Law Review by an authorized editor of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.
DRONES AND DATA: A LIMITED IMPACT ON PRIVACY

David Sella-Villa *

INTRODUCTION

Concerns about drones and their impact on privacy are misplaced. Most of the scenarios discussed in the academic literature and policy commentary simply assume that drones operate in a unique way. These discussions of drones and privacy have left the antecedent question unexamined—precisely how do drones impact privacy? This Article is the first to clearly define the operational parameters of drones that impact privacy in a unique way. From this precise definition, we learn that drones operate in very few spaces that allow them to capture data inaccessible to other technologies. In short, how drones operate has a limited impact on privacy.

Drones, however, are primarily data collection devices. By tracing the flow of data into and from a drone, it becomes clear that many parties potentially have access to drone-captured data. The privacy impact of drones, therefore, must be understood in the light of the third-party doctrine. Once a drone captures data about a person, that person has almost no recourse to prevent its sharing and distribution.

* Interim Chief Privacy Officer, South Carolina Department of Administration, focusing on technology, privacy, and security issues; CIPP/US, CIPP/E, CIPM, and GLEG certifications; Adjunct Professor, William & Mary Law School, aviation law class. J.D., William & Mary Law School; Editor-in-Chief, Environmental Law and Policy Review; M.S., London School of Economics; B.S. & B.A., West Virginia University.

I would like to thank Russ Weinberg, Josh Gupta-Kagan, and Scott Hochberg for invaluable comments on an early draft of this Article. Mike Shelton kindly assisted with the images and graphics. A special thanks to research assistant Jenna Chaudri who helped this piece achieve its potential. Of course, none of this would have been possible without the constant support and encouragement of my wife, Meredith.

The views and opinions expressed in this Article are those of the author in his individual capacity, and do not reflect the opinions, policies, or positions of any his employers or affiliated organizations or agencies.
Drones have also stirred the emotions of legislators. Hundreds of provisions in state and local laws purport to address the privacy concerns presented by drones and their data. This Article analyzes these laws and demonstrates that very few actually address the unique privacy impact of drones and their data flow. Furthermore, these laws interact with the third-party doctrine in a manner that mutes almost all privacy protections. Concerns about the privacy impact of drones, therefore, should focus on either limiting data capture by drones or changing the U.S. privacy doctrines.

I. DESCRIBING THE DRONE PRIVACY PROBLEM PRECISELY

Many scholars and commentators have sought to link the fears inspired by drone usage with legal conceptions of privacy. Some have looked to the emotions stirred by drones to catalyze broad changes to U.S. privacy protections. Others assume the ubiquity of drone operations and suggest “drone operation[s] may destroy[] society’s privacy expectations to the degree that individuals have no reasonable expectation of privacy from drone surveillance.” Military drone technologies that are yet to be widely de-


ployed in U.S. civilian contexts have inspired assertions that government agencies can “watch a person’s movements to and from his or her home at all hours of the day and night without the chance of detection.”

The scenarios described by others simply assume that drones operate in a unique way. Drones, however, are not truly a unique technology. Drones are simply an amalgam of technologies that the Supreme Court has already analyzed for their impact on privacy. In one sense, drones are simply aircraft. The radio controls used to operate them can still be found in drones’ progeny—model aircraft. But because they are unmanned, drones typically come equipped with cameras to allow the operator to see where it is flying. Manned aircraft, and even satellites, have cameras. Cameras are not new—Warren and Brandeis warned about the privacy invading qualities of cameras in the 1890s. Drones, therefore, could be no different than any other camera-equipped technology. If a


5. Scharf, supra note 3, at 460.


8. Farber, supra note 4, at 12.


photo is taken, from a privacy perspective, the platform taking the photo could well be irrelevant. Why then so much concern about drones’ impact on privacy?

Concededly, it makes intuitive sense that drones are different from other technologies. A few have hinted at the precise answer as to exactly how drones are different. John Villasenor, in his seminal piece on drone privacy, described a scenario where “a UAS, hovering in a backyard and taking pictures through a window . . . acquire[s] images that might show an occupant of the house in a state of undress.”11 Michel and Gettinger noted that “[m]any worry that small camera-equipped unmanned aircraft could enable users to fly over or near private property and record data that would not have been accessible by other means.”12

Drones are distinct from manned aircraft because of their combination of minimum safe altitude of lawful operations, maneuverability, required training, operator intent, and detectability.13 The images captured by drones can be distinguished from the capabilities of observers on the ground, manned aerial photography, satellites, and even a neighbor’s elevated vantage points.14 This Article is the first to show that the net impact of these distinguishing characteristics, however, proves to be rather limited.

The flight capabilities of drones have drawn the attention of many privacy commentators.15 But if the unique operational parameters of drones are rather limited, then what feature of drones justifies the claims of significant privacy impacts? This Article uses a definition of drones that emphasizes their most salient feature—drones are primarily data collection devices.

Building on the work of Joseph Vacek, this Article traces how data flows to and from drones.16 The data captured by drones includes images and information about data subjects other than the

13. See infra section III.A.
14. See infra section III.B.
15. See, e.g., supra notes 2–4 and accompanying text; infra note 42 and accompanying text.
Drone software programs nearly automatically share drone-captured data with the drone software provider.\textsuperscript{17} Drone-captured data, therefore, becomes a business record of the drone software provider—a third party.\textsuperscript{18} Once the data becomes a business record of a drone software provider, the third-party doctrine effectively prevents a data subject from stopping the distribution, sharing, or sale of that data with others.

Even without clearly defining how drones can impact privacy, the legislative urge to address privacy issues presented by drones has been strong.\textsuperscript{19} The Federal Aviation Administration (“FAA”)...
has left drone-related privacy issues to states and localities.\textsuperscript{20} The author has identified over 150 drone-specific provisions in dozens of state and local codes that aim to protect the home from unwanted data collection by civilian drone operations.\textsuperscript{21} With the unique privacy impacts presented by drones clearly defined, and the interaction of drone data flows on the third-party doctrine thoroughly discussed, this Article assesses the potential efficacy of these statutes and ordinances.\textsuperscript{22} In other words, do drone-specific state and local laws even have the potential to address the unique privacy problems presented by drones?\textsuperscript{23} 

The Article concludes by discussing the interplay between state and local drone-specific privacy protections and the third-party doctrine. Despite state and local legislative efforts, current privacy jurisprudence and the third-party doctrine present nearly insurmountable barriers for someone seeking to assert a privacy interest in drone-captured data. Drones, even with their unique abilities, did not create these circumstances. Rather, drones and their data flows simply highlight the logical ends of current privacy doctrines in the United States.

To support these claims, this Article operates from a specific definition of the terms “drone” and “drone usage” based on three key assumptions. First, this Article assumes that a civilian operates the drone for her own purposes—not on behalf of a government unit or law enforcement agency. This assumption is based on a the-

\begin{itemize}
\item \textsuperscript{21} This means statutes and ordinances that specifically include the terms “drone” or “unmanned vehicle” or “unmanned aerial” in the provision. The full list of these laws is in the Appendix.
\item \textsuperscript{22} See United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) (“In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.” (citations omitted)).
\item \textsuperscript{23} See Rebecca L. Scharf, Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy, 94 IND. L.J. 1065, 1067 (2019) (suggesting that drone-specific privacy laws give little consideration to the unique features of drones).
\end{itemize}
ory common in privacy jurisprudence that “generally the police officer may do as the citizen would.”24 Related to this idea, the question of who is operating the drone is largely irrelevant to those who might take steps to prevent privacy invasions by drones. Drones are capable of flying in the same airspace regardless of whether a government official or a civilian operates them. Looking at how drones may be operated lawfully by private parties,25 therefore, sets the standard against which people should expect drones to be used even by the government,26 barring some other authorization27 that is consistent with the Fourth Amendment.28

The second assumption is that the civilian operator is flying the drone lawfully. This means that the drone operator flies in compliance with all applicable FAA laws and regulations,29 as well as any state and local laws.30 During such operations the potential impact on privacy becomes relevant. Otherwise, the rules banning unlawful drone operations indirectly serve to protect privacy interests.31

The third assumption is that the drone only has image capture capabilities of the visible light spectrum. The visible light spectrum simply means what is visible to the naked eye.32 This excludes frequencies not visible to the naked eye, such as infrared and ultraviolet, as well as radio frequencies and other electromagnetic fields.33 Most drones come equipped with cameras capable of capturing the visible light spectrum.34 Though drones can carry sensors capable

27. E.g., IDAHO CODE § 21-213.
30. E.g., TENN. CODE ANN. § 39-14-405 (barring aerial trespass by drone).
31. Villasenor, supra note 11, at 473.
33. See, e.g., AVENTURA, FLA., CODE OF ORDINANCES § 30.211(b) (2019).
34. See Brandon Gonzalez, Drones and Privacy in the Golden State, 33 SANTA CLARA HIGH TECH. L.J. 288, 291 (2016).
of acoustical listening or even chemical sensing (olfaction), the privacy impact of these technologies is beyond the scope of this Article.

From these three assumptions about drone operations a sufficiently detailed assessment of the privacy impact of drone operations becomes possible. To make such an analysis meaningful, the definition of “privacy” merits similar consideration. Privacy, though, is notoriously difficult to define. In this Article, unless stated otherwise, “privacy” simply means freedom from unwanted visual observation in and about the home.

Linked to these assumptions about drones, visual observation in the privacy context means observations of the visible light spectrum. Observations of the visible light spectrum have the most developed privacy jurisprudence in the United States. This Article focuses on the home because, in the U.S. legal tradition, privacy expectations and protections are at their highest and strongest in and about the home. The freedom from visual observations of the home ties closely to cases involving technology similar to drones, such as manned, fixed-wing aircraft and helicopters. By establishing how drones might uniquely impinge one's privacy interest in freedom from visual observation in one's most protected space, future discussions about other privacy interests and other technologies become possible by comparison and analogy.

To these ends, Part II defines lawful drone usage for the purposes of this Article while emphasizing the data-capture qualities of drones. Part III distinguishes drones from other aircraft and

36. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) (“Privacy . . . is a concept in disarray.”).
37. See supra note 32 and accompanying text.
39. Id. at 37 (noting “the Fourth Amendment sanctity of the home”).
42. WELLS C. BENNETT, BROOKINGS INST., CIVILIAN DRONES, PRIVACY, AND THE FEDERAL-STATE BALANCE 3 (2014) (“As pressing as the question of how best to safeguard ‘public’ privacy, is the question of how best to safeguard its understudied counterpart, ‘private’ privacy.”).
other image-capture techniques. This way, the unique operational and image-capture qualities of drones, and how data flows through them, can be clearly defined. Part IV presents the preexisting non-drone-specific legal privacy protections in and about the home. By understanding these privacy protections through several different analytical and legal frameworks, the protections extending to drone data may be better understood.\footnote{See United States v. Miller, 425 U.S. 435 (1976); Kaminski, supra note 3, at 66; Blitz et al., supra note 24, at 80.} Taking all these factors into account, Part V articulates the unique privacy impact of drones. Part VI presents categories of drone-specific state and local laws and assesses whether they are capable of protecting against the unique impacts on privacy created by drone use and drone data flows. This Part demonstrates that drones simply highlight the areas where the preexisting legal framework fails to offer adequate privacy protections. The Article concludes with a discussion of what elements of the legal framework might merit reform in light of drones’ unique abilities, and suggestions for future analyses of drones’ impact on privacy.

II. DEFINING DRONE USAGE


For the purposes of this Article, the term “drone” means an aerial vehicle with the following characteristics: (1) it meets the FAA’s
definition of an aircraft;\textsuperscript{50} (2) it is unmanned because it is “operated without the possibility of direct human intervention from within or on the aircraft”\textsuperscript{51} (3) it weighs less than fifty-five pounds;\textsuperscript{52} (4) it can be controlled for the purposes of flight operations and landing;\textsuperscript{53} (5) it is entirely remotely controlled;\textsuperscript{54} (6) it is mounted with a camera-image capture device capable of recording the visible light spectrum;\textsuperscript{55} and (7) the operator can see either in real time or a recording of what the camera on the drone can capture in its field of vision.\textsuperscript{56}

The FAA requires registration of drones weighing over fifty-five pounds in the same manner as a manned aircraft.\textsuperscript{57} Registration of such a drone implicates other FAA regulations that require significant aeronautical knowledge and potentially even an FAA-approved type design of the aircraft.\textsuperscript{58} Acquiring such knowledge


\textsuperscript{51}. FAA Modernization and Reform Act § 331(8).

\textsuperscript{52}. Id. § 331(6).

\textsuperscript{53}. Though the drone may be launched as a rocket, the ability to control it during flight and to control the landing distinguishes drones from most model rockets and untethered balloons. But see RC Lover san, Landing a Rocket Vertically, Without Being a Billionaire Aka Rocket Drone, INSTRUCTABLES: OUTSIDE, https://www.instructables.com/id/Landing-a-Rocket-Vertically-Without-Being-a-Million/ [https://perma.cc/E3M-H7NJ].

\textsuperscript{54}. The FAA includes “tethered UAS” in its definition of UAS, but for the purposes of this Article, drones are distinguished from most kites and other flying contraptions tethered to the ground. See FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 341(a), 132 Stat. 3186, 3284. But see Vidi Nene, Facebook Patents Dual Kite Aerial Vehicle, DRONE BELOW (June 4, 2019), https://dronebelow.com/2019/06/04/facebook-patents-dual-kite-aerial-vehicle/ [https://perma.cc/TQ8P-E2ZM].

\textsuperscript{55}. See Scharf, supra note 23, at 1080. This Article will only focus on image capture capabilities. In the field of audio capture, wiretap laws offer technology-neutral protections against certain audio recordings of the home. As other scholars have noted, these laws can likely be applied to the audio recording capabilities of unmanned aerial vehicles. See Kaminski, supra note 3, at 65–66; Villasenor, supra note 11, at 498. Additionally, many state and local laws explicitly include unconsented audio recordings in the list of improper drone uses. E.g., CAL. CIV. CODE § 1708.8(f)(1) (West 2016). An interesting application of wiretap statutes would arise in a scenario where a drone captures video footage of a person speaking American Sign Language. See, e.g., Michael F. Kelleher, Comment, The Confidentiality of Criminal Conversations on TDD Relay Systems, 79 CALIF. L. REV. 1349 (1991).

\textsuperscript{56}. Scharf, supra note 23, at 1102. Additionally, many drone-specific state and local laws specifically mention drones’ recording capabilities. E.g., LA. STAT. ANN. § 14:283.3 (2018); IND. CODE § 35-45-4-5(g) (2020).

\textsuperscript{57}. See FAA DroneZone, FED. AVIATION ADMIN., https://faadronezone.faa.gov/ (https://perma.cc/4UAIJ-PRZ5) (“You must use the paper (N-number) registration process if your unmanned aircraft is 55 pounds or greater.”).

\textsuperscript{58}. 14 C.F.R. § 47.33 (2020).
and obtaining FAA-type design approval is the purview of manned aircraft. Any discussion about drones’ impact on privacy that requires a drone that weighs more than fifty-five pounds is effectively a discussion about manned aircraft. Accordingly, concerns about the capabilities of drones that weigh more than fifty-five pounds should be addressed through privacy jurisprudence related to manned aircraft. The privacy impact of drones should focus on those devices that are not treated like manned aircraft.


The definition of “drone” used in this Article incorporates both the small UAS (“sUAS”) and the model aircraft terms used by the FAA. This Article simply uses the term “drone” to refer to a device with all the above-mentioned features, regardless of whether the FAA would consider it an sUAS or a model aircraft. Though the distinctions between sUAS and model aircraft operations are important for drone operators to consider, lawful operations of both are sufficiently similar that they can be discussed together for the purposes of understanding the unique privacy impact of drones.

Federal Aviation Regulations under Part 107 and the FAA’s model aircraft rules share several common provisions. Lawful operations for both classifications of aircraft require that the drone operates (1) within the visual line of sight of the person operating the aircraft or a visual observer co-located and in direct communication with the operator; (2) in Class G airspace; (3) below 400 feet; (4) in a manner that does not endanger people or property on the ground; (5) by an operator who has passed an aeronautical knowledge test; and (6) by an operator, if not the drone as well, that is registered with the FAA. Upon application and approval, the FAA can authorize drone operations that would otherwise violate these rules.

Currently, the FAA only allows operations of drones over people after both the drone and the operator meet extensive requirements. Importantly, under this set of conditions, a drone operator can lawfully fly over her own property up to an altitude of 400 feet. Depending on the state or locality, the drone operator may

---

67. See Villasenor, supra note 11, at 474–75; Blitz et al., supra note 24, at 71 n.107 (“What matters is not merely that a particular technical device or system is not overly unusual, but that its use in a particular context, in a particular way is not overly unusual.”
even be able to operate the drone so that it may cross a neighbor’s terrestrial property line lawfully.68

Drone sales exploded once lighter materials and better algorithms made both flight controls and image capture very easy for even the least experienced drone operators.69 If a drone operates without a camera capable of recording, then it is no different than the model aircraft enjoyed by model aeronautics enthusiasts and has no impact on the privacy interests discussed in this Article. People primarily operate drones not for their flying abilities,70 but rather for their data collection abilities.71 Some drones even allow the operator to preprogram a flight path so the operator can focus solely on image capture.72 Put concisely, drones are “simply the platform for enabling surveillance.”73 In this Article, the data in question is the images captured by the camera on the drone. Before

---


70 The AMA is the largest model aircraft organization in the world. See supra note 62. If drones were operated simply for the operator to enjoy their flight, then the recent explosion in drone sales would have been reflected by significant growth in AMA membership. See Marcus Chavers, Consumer Drones by the Numbers in 2018 and Beyond, NewsXledge (Oct. 13, 2018), https://www.newsledge.com/consumer-drones-2018-numbers/ [https://perma.cc/4AHH-PW6W], Fact Sheet—The Federal Aviation Administration (FAA) Aerospace Forecast Fiscal Years (FY) 2020-2040, Fed. Aviation Admin. (Mar. 26, 2020), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=24756 [https://perma.cc/3JA2-T4K9]. That simply did not occur. Even with millions of drones sold, AMA membership has stayed relatively constant. Compare Modelaircraft, AMA Air at 1:38, YouTube (Dec. 1, 2016), https://www.youtube.com/watch?list=PLYA5FHbSdqot9Tkxk-dKPc8NUJJJaW1nxb&v=RnGdGa5EdQQ [https://perma.cc/9GJR-HG63] (“What took ground teams 6 months to inspect, took PrecisionHawk’s drone operators and data analysts just 6 weeks.”); see Vacek, supra note 2, at 465; Farber, supra note 4, at 12.

71 E.g., PrecisionHawk, Enriching Data, Empowering Action 8 (2020), https://www.precisionhawk.com/hubfs/PrecisionHawk_Encirhing%20Data,%20Empowering%20Action_Whitepaper.pdf [https://perma.cc/l6V8-2YLM] (“What took ground teams 6 months to inspect, took PrecisionHawk’s drone operators and data analysts just 6 weeks.”); see Vacek, supra note 2, at 465; Farber, supra note 4, at 12.

72 Miller, supra note 1, at 353.

73 Hillary B. Farber, Keep Out! The Efficacy of Trespass, Nuisance and Privacy Torts as Applied to Drones, 33 GA. St. U. L. Rev. 359, 370 (2017); accord Scharf, supra note 3, at 458.
discussing drone image capture any further, it is necessary to distinguish drones from other aviation and image-capture technologies.

III. DISTINGUISHING DRONES FROM OTHER AIRCRAFT AND IMAGE-CAPTURE TECHNOLOGIES

This Part explains why drones are distinct from other flying machines and image-capture technologies. Through these distinctions, this Part will demonstrate that drones offer an image-capture perspective akin to the elevated vantage points on neighboring properties. This Part concludes by distinguishing drones from these fixed vantage points on neighboring properties.

A. Distinguishing Drones from Other Flying Machines

Drones are aircraft. The definition of drones used in this Article already distinguishes them from rockets, balloons, kites, and other tethered flying machines. As aircraft, drones are distinct from other manned flying machines liked fixed-wing aircraft (airplanes), rotary-wing aircraft (helicopters), and non-steer aircraft (hot air balloons). Though drones that make visual observations of the ground have elements in common with each of these flying machines, no other aircraft has the same combination of the following characteristics: minimum safe altitude of lawful operations, maneuverability, required training, operator intent, and detectability. Because of this combination of features drones can capture images of the ground from vantage points and at a frequency inaccessible to other flying machines.

1. Minimum Safe Altitude of Lawful Flight Operations

The more an aircraft weighs, the more gravity’s pull beckons. In defining the minimum safe altitudes for operation, the FAA requires that all types of manned aircraft (fixed-wing, rotary-wing, and hot air balloons) always operate at “[a]n altitude allowing, if a power unit fails, an emergency landing without undue hazard to
persons or property on the surface." 76 In practical terms, once an emergency situation commences, 77 the aircraft operator needs enough time to try and steer the aircraft towards a location that will minimize damage to the aircraft (and accordingly its pilots and passengers), as well as people and objects on the ground. 78

These altitude regulations reflect the FAA’s safety mandate. 79 The FAA’s Center of Excellence study determined that if a drone falling from the sky generates more than fifty-five foot-pounds of energy, approximately seventy-five Joules, a lethal head injury can occur about fifty percent of the time. 80 To achieve this quantum of energy, a drone weighing about five pounds would have to free fall from 400 feet. 81 The potential lethality of heavier drones falling from lower altitudes can be extrapolated accordingly. Since the FAA began keeping records of drone safety incidents, though, there have been no drone-related fatalities. 82

Because manned aircraft weigh hundreds, if not thousands, of times more than drones, 83 they cannot lawfully operate at such low altitudes. Under normal operating conditions, any manned aircraft flying over a populated area needs to keep a minimum altitude of 1000 feet. 84 In contrast, drones are only allowed to operate up to

76. 14 C.F.R. § 91.119(a) (2020).
78. 14 C.F.R. § 91.13 (2020).
81. Arterburn et al., supra note 80, at 47.
83. Arterburn et al., supra note 80, at 47.
84. 14 C.F.R. § 91.119(b) (2020).
400 feet. If a manned aircraft happens to be operating at 400 feet lawfully, it would only be during take-off, landing, or in an emergency situation. Under any of these circumstances, the focus of the aircraft operator should not be on taking pictures or video. But a drone operator can operate at those altitudes and be focused on taking pictures or video.

For these reasons, drones can be distinguished from all manned aircraft because they can operate lawfully and safely for the purpose of image capture at much lower altitudes. Any discussion of the privacy impact of drones that suggests that the drone can operate above 400 feet fails to distinguish drones from manned aircraft. If a drone happens to operate above 400 feet, it is in the territory of manned aircraft and their associated privacy jurisprudence. The unique privacy impact of drones, therefore, can only be understood if the drone operates below 400 feet.

2. Maneuverability

The most popular drones have a “quadcopter” design. Quadcopters, like manned helicopters, can both travel laterally and hover

---

85. *Id.* § 107.51(b).

86. *See* FED. AVIATION ADMIN., *supra* note 77.


in one spot in the air without moving laterally or vertically.\textsuperscript{89} Fixed-wing aircraft achieve lift by moving air over the airfoil of the wing, necessitating lateral movement of the aircraft both for take-off and at all times when traveling through the air.\textsuperscript{90} A fixed-wing aircraft, therefore, cannot hover. For this reason, the maneuverability of drones is distinct from that of fixed-wing aircraft.\textsuperscript{91}

The FAA deems hot air balloons “a nonsteerable aircraft.”\textsuperscript{92} Steering is a necessary component of maneuverability. Drones are remotely controlled,\textsuperscript{93} implying steering control at all times, and are therefore steerable aircraft. Accordingly, drones can be distinguished from fixed-wing aircraft and hot air balloons because they are more steerable and maneuverable.

Two key factors distinguish the maneuverability of drones from that of helicopters. Quadcopter drones are designed for a near vertical take-off,\textsuperscript{94} while this maneuver at a similar angle cannot be achieved in civilian helicopter operations.\textsuperscript{95} Helicopters can operate at some of the same altitudes as drones but only with FAA permission on a strictly preset flight path.\textsuperscript{96} Simply due to their massive size differences, though, helicopters would not be able to fly as safely near obstacles on the ground as drones.

Specifically, all aircraft must fly at a minimum altitude that allows for as safe a landing as possible in the event of engine failure.\textsuperscript{97} To meet this safety standard, helicopters must attempt to fly
into the wind when operating at low altitudes. The winds in and around obstacles on the ground, like buildings and trees, are irregular, making lawful helicopter operations (with the exception of take-off and landing) at such low altitudes nearly impossible. Because helicopters have a more limited set of operating conditions in which they safely and lawfully gather information, drones can be distinguished from helicopters based on maneuverability. This allows drones to capture images of the ground otherwise inaccessible to helicopters.

3. Required Training

All manned aircraft pilots require extensive training before they can operate such aircraft alone. In addition to qualifying medically and completing classroom training, manned aircraft pilots must pass written exams, accumulate training flights hours in the air, and pass a check ride with an FAA official. All of these steps aim to impress the importance of safety and proficiency in all new pilots. Costs aside, the time invested in becoming a licensed pilot represents a barrier to entry that fewer overcome each year.

No training is required to operate a drone. Though drone operators must pass an aeronautical knowledge test, these assessments do not test the drone operator’s actual ability to control the drone safely during flight. One could pass the test even before having access to a drone. Drone manufacturers specifically make

99. Id. at 10-10.
104. See FED. AVIATION ADMIN., REMOTE PILOT—SMALL UNMANNED SYSTEMS STUDY GUIDE (FAA-G-8082-22), at iii–v (2016) (listing the topics on remote pilot exam, not including questions about how to operate a drone).
them very easy to fly with no training by allowing for flight controls through a mobile phone app. Taken to its comedic, albeit fictional, extreme, even one-handed Buster Bluth can operate a drone as if it were an arcade game. The number of remote pilot certificate holders has increased by roughly 40,000 each year since the certification was offered. Training, accordingly, is not a barrier to access for civilian drone operations.

It is important to remember that drones discussed in this Article must be flown within the visual line of sight of the operator. Much like the differences between visual flight rules and instrument flight rules for manned aircraft, drone operators must rely on sophisticated instruments to fly drones beyond the visual line of sight (“BVLOS”) of the drone operator. With few exceptions, U.S. drone BVLOS operations have been reserved almost exclusively for military and search-and-rescue operators. Safely flying drones in BVLOS conditions requires an extensive flight program. Accordingly, discussions of the privacy impact of drones

105. Scharf, supra note 23, at 1073.
106. See Fisher, supra note 88.
109. See supra note 62.
114. Kansas State University Polytechnic Campus’s Applied Aviation Research Center has received at least two BVLOS waivers from the FAA in part because, as articulated by Kurt Carraway, the head of the Research Center, “our ability to conduct thorough operational risk assessments and articulate those into safety cases...to garner FAA approval for advanced UAS operations.” K-State Polytechnic Campus Receives Waiver to Fly UAS BVLOS in All Class G Airspace Nationwide, AUVSI NEWS (Aug. 17, 2020), https://www.auv
that suggest BVLOS operations assume a type of drone operation that simply does not take place with any regularity. Drones that operate BVLOS, therefore, require investment in operational resources akin to manned aircraft.

For these reasons, drones are completely distinct from manned aircraft in terms of their training requirements. This means that more people have the possibility to operate drones for the purpose of image capture than pilots flying manned aircraft for the same reason.

si.org/industry-news/k-state-polytechnic-campus-receives-waiver-fly-uas-bvlos-all-class-g-airspace [https://perma.cc/9CDK-A2PT].

115. See Farber, supra note 4, at 7; Goldstein, supra note 87; Schlag, supra note 3, at 12; Joseph J. Vacek, Big Brother Will Soon Be Watching—Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement, 85 N.D.L.R. REV. 673, 674 (2009) (suggesting persistent drone operations that require BVLOS operations); Mara, supra note 60, at 3–5; Alexandria Tomanelli, A Drone’s Eye View: Why and How the Federal Aviation Administration Should Regulate Hobbyist Drone Use, 34 TOURO L. REV. 867, 877, 879 (2018); Nolan, supra note 87, at 1459; Talai, supra note 60, at 745–46; McNeal, supra note 60, at 406–07; Spelman, supra note 60, at 379, 400, 411; Farber, supra note 2, at 6; Ragatzki, supra note 60, at 199; Reid, supra note 60, at 8, 65; Derek Larson & Patrick S. Roberts, How Two Traditions of Privacy Defenses in Image Capture Technology Inform the Debate Over Drones, 13 I/S: J.L. & Pol’y for Info. Soc’y 465, 487 (2017); Mark G. Huffman, Note, “Honey, There’s a Drone on the Lawn”: Assessing the Supreme Court’s Unspoken Perspective on the Future of Drones in the Commercial Industry, 18 WAKE FOREST J. BUS. & INTELL. PROP. L. 143, 145 (2017); Black, supra note 60, at 1831, 1840; Gray & Citron, supra note 60, at 106; Suominen, supra note 60, at 39; Molko, supra note 60, at 1286; Gavrilovic, supra note 60, at 550; Jenks, supra note 60, at 1400; Crotty, supra note 60, at 227; Jennifer Daskal, The Un-Territoriality of Data, 125 YALE L.J. 326, 370 (2015); Barbee, supra note 2, at 468–69; Rapp, supra note 60, at 644.

4. Operator Intent

Most civilian drones have an electric motor\textsuperscript{117} that uses batteries as a power supply.\textsuperscript{118} At full charge, they only stay in the air for a few minutes.\textsuperscript{119} A drone operator will spend at most a few cents to fully charge a drone battery.\textsuperscript{120} These low operating costs mean that drone operators can fly them intermittently with little preparation.

Nearly all manned aircraft use fuel combustion to generate power.\textsuperscript{121} Airplanes and helicopters consume crude oil derivatives known as Jet Fuel and Avgas.\textsuperscript{122} Like gasoline, their prices change regularly. As of the writing of this Article, fuel prices at southeastern Virginia airports ranged from $3.39 to $7.08 per gallon.\textsuperscript{123} Using a Cessna 172, the most popular small, manned aircraft in the United States,\textsuperscript{124} can help illustrate the massive difference in operating costs between manned aircraft and drones.

A 1997–2007 Cessna 172R has a fuel capacity of fifty-six gallons and a fuel burn rate of about 8.6 gallons per hour.\textsuperscript{125} Assuming a

\begin{itemize}
\item \textsuperscript{117} See Olivito, supra note 3, at 676.
\item \textsuperscript{118} See Joe Pappalardo, New Lithium Metal Batteries Can Power Drones for Longer (and It Could Change Everything), POPULAR MECHS. (Apr. 16, 2019), https://www.popular-mechanics.com/flight/drones/a27155551/battery-boeing/ [https://perma.cc/TF36-L4H8].
\item \textsuperscript{119} See id.
\item \textsuperscript{122} See Focus on Fuel Part One: Different Types of Aviation Fuel, JETEX, https://www.jetex.com/focus-fuel-part-one-different-types-aviation-fuel/ [https://perma.cc/TBC7-RVRR].
\end{itemize}
price of $5.00 per gallon for fuel, this means a Cessna pilot would spend about $280 for six hours of flight time.\textsuperscript{126} Fuel costs, though, represent only a tiny fraction of the financial considerations involved in owning and operating a manned aircraft.\textsuperscript{127} A manned aircraft can stay in the air much longer than a drone, but the cost of getting it there is immensely greater. This suggests that pilots operate manned aircraft with much more specific intentions than drone operators.

Drones operate primarily to make visual observations of the ground through their cameras.\textsuperscript{128} Aircraft primarily operate to transport people and cargo,\textsuperscript{129} but can also be used to make visual observations. Even when a pilot flies a manned aircraft specifically to make visual observations of the ground,\textsuperscript{130} she demonstrates much more intentionality than a drone operator.

The camera found on a drone is typically attached to a gimbal.\textsuperscript{131} The gimbal prevents the camera from vibrating during flight, allows the camera to move independently of the drone, and adjusts the camera automatically through the drone operations software program.\textsuperscript{132} This means that a drone will nearly automatically capture focused images of objects on the ground. Simply by operating the drone, even without specifically intending to do so, the drone operator enjoys detailed visual observations of the ground.


\textsuperscript{127} See \textit{Hypothetical Operating Cost Calculation}, AOPA, \url{https://www.aopa.org/go-fly/aircraft-and-ownership/buying-an-aircraft/tips-on-buying-used-aircraft/hypothetical-operating-cost-calculation} \[https://perma.cc/SM2T-MTL2\]. Acquirers of civilian drones will spend a fraction of what the purchase price of even a used manned aircraft would cost. See Scharf, \textit{supra} note 3, at 466. Because this discussion focuses on drone operations, purchase costs are not pertinent.

\textsuperscript{128} See \textit{supra} notes 55–56 and accompanying text.

\textsuperscript{129} See Blitz et al., \textit{supra} note 24, at 54, 66.


\textsuperscript{131} See Fisher, \textit{supra} note 88.

To achieve the same quality of images from a manned aircraft, the operator would need costly, specialized, photographic equipment. Aircraft used primarily for aerial photography have a restricted airworthiness certificate that limits their operations. Accordingly, the specific intention to capture images of the ground is set at the moment of aircraft purchase. To install such equipment on a civilian manned aircraft after purchase requires a similar level of intent because such installation requires special permissions from the FAA through its supplemental type certificate process. To get as close as possible to a drone-quality photograph with a manned aircraft, a gimbal would have to be attached to a helicopter. Helicopter operating costs exceed those of a fixed-wing aircraft.

The intent required for a manned aircraft to capture images of the ground also affects the lifecycle of those images. Companies like EagleView (formerly Pictometry) use manned aircraft to capture images of the ground and license those images for a fee. Bing Maps, for example, used photos from Pictometry to populate some images of its Bird’s Eye View. These images are only shared pursuant to contractual terms that protect EagleView’s intellectual property rights and economic interests. This means that those who share images captured from manned aircraft do so very intentionally.

The lifecycle of civilian drone-captured images is very different. As described eloquently by Joseph Vacek, the drone “data chain contains four links: (1) drone operation itself, (2) in-flight data col-

133. See infra section III.B.
136. Id. §§ 21.111–.119.
lection, (3) post-flight data processing, and (4) data use, dissemination, and storage.”

Visual observations made by drones are covered in links two through four of the data chain. Once the data leaves the drone and its operating software begins processing it, it is likely the captured images themselves have effectively been shared with the drone software provider making them a business record of the drone software provider. This means that simply by flying the drone, the drone operator has shared the images. The level of intent needed to share drone-captured images, therefore, is much lower than that of manned aircraft.

With all these factors combined, capturing visual observations from a manned aircraft requires a very high level of intentionality—to capture images, by having specialized equipment installed on an aircraft, that is expensive to operate. For a drone, the level of intention required for detailed observations of the ground is achieved merely by deciding to operate the drone. Additionally, images captured from manned aircraft are shared very intentionally. That same level of intent is utterly absent in the process of sharing drone-captured images. The degree of difference is so great that it is effectively a different kind of intent. Accordingly, drone image capture can be differentiated from manned aircraft based on the differences in operator intent.

5. Detectability

A person not operating a drone would hopefully be able to detect the presence of a drone through either visual or auditory cues.

140. Vacek, supra note 7, at 139.
141. See supra note 17.
142. See Aldrich, supra note 18, at 5.
143. See Kevin S. Bankston & Ashkan Soltani, Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones, 123 YALE L.J. ONLINE 335, 330–40 (2014) (building on Justice Alito’s concurrence in U.S. v. Jones, arguing that massive differences in cost scales differentiate surveillance technologies to such a degree that the resulting searches should be treated differently for Fourth Amendment purposes).
144. Most people also enjoy use of their senses of smell, touch, and taste. By the time someone could use any of those senses to detect a drone, hopefully she would have heard it or seen it first. But see WW2 People’s War: North London During the Blitz, BBC (Nov. 4, 2003), https://www.bbc.co.uk/history/ww2peopleswar/stories/01/a1965701.shtml [https://perma.cc/6BXZ-7ZE9] (“The incendiary bombs were far more insidious. You couldn’t hear these coming . . . ” (emphasis added)).
Most drones produce sounds as loud as eighty decibels. Decibels are measured on a logarithmic scale—every ten decibels reflect a doubling of “loudness.” For comparison, from a distance of 100 feet a helicopter produces about 100 decibels, making it at least four times as loud as a drone. To a person located outdoors, these drones sound about as loud a small aircraft flying at 1000 feet or a passenger car fifty feet away traveling at sixty-five miles per hour. But even the noisiest drones would not sound this loud because operations over people are limited by regulations, so the drone would have to operate at some safe distance. Drones would sound even quieter to someone inside a home.

The quietest drones produce only about sixty decibels of sound. Background music or a normal conversation from a distance of three feet sounds this loud. This is between one-half and one-quarter as loud as a normal drone. If someone were in a home and a quiet drone flew by, only the relative novelty of the sound might alert her to the drone’s presence. Though drones are not auditorily undetectable, they make relatively little noise, especially when compared to manned aircraft.

Assuming someone who is not operating a drone hears it, then she would have to make visual contact with it to determine what images it might be capturing. From a visual perspective, drones...
are a mere fraction of the size of manned aircraft.\textsuperscript{154} It is harder to see a smaller thing than a larger thing. Fixed-wing aircraft and helicopters only regularly operate at low altitudes during take-off and landing, but people within those flight paths would have notice of the aircrafts’ presence.\textsuperscript{155}

Drones are not allowed to operate in the same airspaces as manned aircraft,\textsuperscript{156} so the chance of seeing an airplane or helicopter operating at the same altitude as a drone would be very slim. Even though hot air balloons, for short periods of time, can lawfully travel at low speeds and low altitudes similar to drones in flight,\textsuperscript{157} their massive size\textsuperscript{158} would likely alert someone to the hot air balloon’s presence. These factors combine to make drones operating for the purpose of image capture far less visually detectable than manned aircraft.

Aside from the fact that drones are smaller and quieter than manned aircraft, all manned aircraft must display their FAA registration numbers conspicuously.\textsuperscript{159} If a manned aircraft were being operated for the specific purpose of making visual observations of the ground, it would hover or fly in a regular pattern at a low altitude.\textsuperscript{160} Because of the display requirements for its registration number, someone on the ground could learn about who is operating
the manned aircraft. This makes spotting a manned aircraft conducting visual observations tantamount to learning who is doing the observing.\footnote{See Dow Chem. Co. v. United States, 476 U.S. 227, 241–42 (1986) (describing Dow’s process of tracing aerial photographs based on FAA registration numbers).} Merely detecting a drone’s presence, though, does not alert the observed to who is doing the observing.

Even if the drone is flying over a neighbor’s property and making observations in the area, it is only a presumption that the neighbor is in fact operating the drone.\footnote{\textit{E.g.}, Myles Ma, \textit{Lower Township Man Admits to Firing Shotgun at Drone}, NJ.COM (Jan. 16, 2019), https://www.nj.com/news/2016/02/lower_township_man_admits_to_firing_shotgun_at_dro.html [https://perma.cc/ZTG6-NKRX] (assuming his neighbor was operating the drone when in fact it was another person).} There are only a handful of ways that someone can learn who is operating a drone. First, the drone operator could let people nearby know about the drone’s operation and associated image capture.\footnote{This would be consistent with the NTIA’s voluntary best practices regarding drone privacy. NAT’L TELECOM. & INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY 8 (2016). Because these recommendations are voluntary, there is no means at the federal level for directly enforcing this practice upon drone operators.} Second, someone could make a direct observation of the person operating the drone.\footnote{Assuming, per note 62 and accompanying text, the drone operator is maintaining the drone within visual line of sight. \textit{But see, e.g.}, Sam Lewis, \textit{FAA Grants Skyward Staff Permission to Conduct BVLOS Infrastructure Inspections from Their Homes}, COM. DRONE PROF. (Sept. 25, 2020), https://www.commercialdroneprofessional.com/faa-grants-skyward-staff-permission-to-conduct-bvlos-infrastructure-inspections-from-their-homes/ [https://perma.cc/4HX5-52N60].} To do so lawfully, the observer would have to locate the drone operator without trespassing or violating any other laws.\footnote{See \textit{Fed. Aviation Admin., Drone Law Enforcement Response} 1 (2018) (instructing local law enforcement officers to “attempt to locate” the drone operator by looking at windows, balconies, and rooftops).} Third, after discovering a drone’s identifying numbers, an inquiry could be made to the FAA as to who is the drone’s registered owner, and accordingly, narrow the search for the possible drone operator.

All drones must have an FAA registration number on them.\footnote{14 C.F.R. § 107.13 (2020).} Only a handful of FAA staffers have access to the database which links drone registration numbers to the names of registrants.\footnote{\textit{E.g.}, U.S. GOV’T ACCOUNTABILITY OFFICE, \textit{supra} note 82, at 11.} Staffers only query the database upon request from government investigators or law enforcement officers.\footnote{\textit{Id.} at 17–18.} Accordingly, upon
learning a drone’s registration number, an occupant would have to engage a law enforcement officer or FAA investigator to make an inquiry to the FAA to identify the registrant.

There are several ways to learn a drone’s registration number. The occupant could read the registration number after bringing it to the ground by disabling it, thereby committing a variety of possible crimes, including violating the Aircraft Sabotage Act. Similarly, the drone could fall to the ground (not land) on another’s property, thereby operating unsafely contrary to FAA regulations.

The new Remote ID regulation provides another avenue to possibly learn the operator of drone. Under Remote ID, a person on the ground would be able to access a broadcast of some information from the drones operating in the area—including either the drone’s serial number or session ID for a particular flight by a drone and “an indication of the control station’s latitude[,] . . . longitude [and] barometric pressure altitude.” The occupant would have to record the information during the course of the broadcast and travel to the control station. But without a grounded drone, it may be more difficult to persuade local law enforcement to query to FAA to identify the drone’s registered owner. In an effort to identify a drone operator, therefore, the most Remote ID can do is potentially narrow the search.


Even after identifying the drone’s registered owner, independent evidence would still be needed to indicate who was operating the drone. The FAA itself has declined to prosecute registrants of drones operating illegally because drone registration does not prove who was actually flying the drone at any specific time.\textsuperscript{173} All told, barring an operator’s voluntary disclosure or direct observation of the drone operator, it is very difficult for an occupant to learn who is making observations of her property.

For these reasons, drones are far less detectable than manned aircraft\textsuperscript{174} and, when all parties behave lawfully, effectively undetectable for the purpose of determining who is using them to make visual observations.

B. \textit{Distinguishing Drones from Other Aerial Imaging Technologies}

Aerial imaging is part of the field of remote sensing. Because this Article focuses on visual observations,\textsuperscript{175} the sensor in question is a camera capable of capturing the visible light spectrum. Manned aerial photography and satellite imaging are the most common remote sensing technologies.\textsuperscript{176} Civilians’ most common means of access to these images—Google Earth and Bing Maps—provide a framework for distinguishing drone-captured images from other remote sensing technologies.\textsuperscript{177} Remote sensing practitioners differentiate images captured from various technologies using several key criteria: swath, nadir point, and resolution. Using these criteria, it is possible to distinguish images captured by


\textsuperscript{174} Scharf, \textit{supra} note 23, at 1080; Hendricksen, \textit{supra} note 60, at 215; Jenkins, \textit{supra} note 2, at 163, 171; Dunlap, \textit{supra} note 87, at 173, 180–81, 201; Nagy, \textit{supra} note 87, at 138.

\textsuperscript{175} See \textit{supra} notes 32–35 and accompanying text.


\textsuperscript{177} See Blitz et al., \textit{supra} note 24, at 75.
drones from those captured by other technologies. These differences reveal that the image capture qualities of drones are most similar to what a neighbor might see from elevated vantage points on her property. Several features differentiate drones from image capture vantage points on a neighbor’s property. Before delving into all these distinctions, below is a quick overview of the relevant remote sensing terms.

1. Key Terms in Remote Sensing

The device that captures the desired images is called the sensor. The sensors discussed here are simply visible light cameras attached to a platform: drone, manned aircraft, or satellite. The field of view is “the angular cone of visibility of the sensor and determines the area of the earth’s surface, which is ‘seen’ from a given altitude.” The total area within a field of view is known as a swath. The nadir point is the imaginary point that touches the earth when “a perpendicular line [is drawn] from the sensor to the ground.” If the sensor is pointed at the earth at other than a perpendicular angle relative to its platform, this is called oblique or off-nadir viewing. The degree of oblique viewing is called angle of view. Swath size increases as the altitude from the sensor to the earth increases or angle of view becomes more oblique.

Once an image is captured, its resolution can be distinguished in four ways. Spectral resolution refers to the range of the electromagnetic spectrum captured by the sensor. For the purposes of

178. The imaging technologies discussed in this section are only those available to civilians. United States law enforcement agencies, other government agencies, and the military have access to much more advanced surveillance aircraft and satellite imaging technologies. See Patrick Korody, Note, Satellite Surveillance Within U.S. Borders, 65 OHIO ST. L.J. 1627, 1627 (2004); State v. Brossart, No. 32-2011-CR-0049, slip op. at 5–6 (D.N.D. July 31, 2012) (describing the North Dakota sheriff’s use of a Predator drone with infrared capabilities operated by the U.S. Department of Homeland Security). The use of government technologies is beyond the scope of analysis of this Article.

179. BUSADEB BHATTA, REMOTE SENSING AND GIS 53 (2d ed. 2011).

180. Id. at 51.

181. Id. at 52.

182. Id.


184. BHATTA, supra note 179, at 55.
this discussion, the spectral resolution in question is the visible light spectrum.\textsuperscript{185} \textit{Radiometric resolution} describes a sensor’s “ability to discriminate very slight differences in energy.”\textsuperscript{186} It is expressed in base 2, so an 8-bit radiometric resolution would generate $2^8$ (256) energy frequencies, i.e., shades of color. High radiometric resolutions do not necessarily generate “better” images in humans’ eyes because our ability to differentiate among shades is rather limited, particularly in grayscale.\textsuperscript{187}

Most relevant for this discussion are spatial resolution and temporal resolution. \textit{Spatial resolution} describes the amount of detail visible in an image by referring “to the size of the smallest possible feature that can be detected.”\textsuperscript{188} It is expressed as the area on the ground—ground sampling distance (“GSD”)—found in the smallest \textit{resolution cell}, or pixel, of an image. For example, a GSD of 2.6 centimeters per pixel allows for the clear reading of the lettering in a parking lot from an altitude of 180 feet.\textsuperscript{189} \textit{Temporal resolution} refers to the frequency with which a sensor “records imagery of a particular area.”\textsuperscript{190} Temporal resolution is expressed in units of time.

2. Distinguishing Swath Size and Field of View

Drones operate differently than manned aircraft.\textsuperscript{191} Drones’ cameras often come mounted on gimbals which allow for motion of the camera independent from the motion of the drone.\textsuperscript{192} This means that the drone camera can have a field of view other than perpendicular from the drone to the ground. This oblique sensing can be achieved with manned aircraft and satellites as well. But, because drones can lawfully operate at much lower altitudes, a drone’s swath will be smaller than that of a manned aircraft or a

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{185} \textit{Tour of the Electromagnetic Spectrum}, NASA SCI., https://science.nasa.gov/ems/09_visiblelight [https://perma.cc/2ZES-9UNL].
\item \textsuperscript{186} \textit{Bhatta, supra} note 179, at 56.
\item \textsuperscript{187} \textit{Id.} at 56–57.
\item \textsuperscript{188} \textit{Id.} at 53.
\item \textsuperscript{189} \textit{Resolution: Understanding Resolution}, DRONEDEPLOY, https://support.dronedeploy.com/docs/resolution [https://perma.cc/7PXW-LL5F].
\item \textsuperscript{190} \textit{Bhatta, supra} note 179, at 58.
\item \textsuperscript{191} \textit{See supra} section III.A.
\item \textsuperscript{192} \textit{See supra} notes 131–32 and accompanying text.
\end{enumerate}
\end{footnotesize}
satellite. A smaller swath increases the probability of a better spatial resolution—allowing for more detailed images.\textsuperscript{193}

The ability for a drone to operate at lower altitudes dramatically shifts the field of view of its sensor. An example helps illustrate the significant difference between the field of view of a drone’s camera and those of manned aircraft and satellites. A drone can hover over a neighboring property at the exact height of someone’s window, all while avoiding trespass.\textsuperscript{194} See Figure 1 below. Because of its gimbal, the operator can direct the drone’s camera to make a visual observation through the window. The field of view of the drone camera would include the far wall of the room visible through the window. With just a little practice\textsuperscript{195} the drone operator could take advantage of the drone’s maneuverability and shift the field of view of the camera around the room.\textsuperscript{196}

Figure 1—Drone, Avoiding Trespass, Flying at Same Altitude as Neighbor’s Windows\textsuperscript{197}


195. \textit{See supra} section III.A.3.

196. \textit{See supra} section III.A.2.

The same geometry of image capture is not available to manned aircraft or satellites. Even if a manned aircraft had a gimbaled camera and an unimpeded view of the same window, the FAA requirements to keep at least 1000 feet of vertical distance and at least 2000 feet of horizontal distance from the tallest structure\(^\text{198}\) would make it nearly impossible to fly at an altitude allowing its angle of view to match that of the drone. A manned aircraft might be able to capture an image that includes the window, but it would have a much more limited field of view of the interior of the room.\(^\text{199}\) A satellite would have an even more difficult time capturing an unimpeded view inside the window because of the incredible distance from its sensor to the interior of the room. Even if a satellite could match the angle of view of a drone looking inside a window, the resolution of the image would be severely diminished because of the increased swath size at such an oblique angle.\(^\text{200}\)

For these reasons, the swath size and nadir point of images captured by drones make them fundamentally distinct from those captured by manned aircraft and satellites.

3. Distinguishing Drone Images from Other Publicly Available Images

Internet-based services such as Google Earth and Bing Maps make images of people’s homes publicly available. These images can be distinguished from drone-captured images in several ways. The imagery on Google Earth and Bing Maps “is actually a mosaic of many images from different time periods, different spatial resolutions (15 m [meter] to 10 cm [centimeter]) and multiple image providers.”\(^\text{201}\) For views of the United States, most of the satellite images are captured from the NASA/USGS Landsat 8 satellite\(^\text{202}\)

199. See Green et al., supra note 183, at 57–60.
200. See id.; Wang et al., supra note 183, at 342.
which offers at best a fifteen-meter GSD spatial resolution. Drones also offer a vastly superior spatial resolution compared to publicly available satellite images. At about fifty feet of altitude, a DJI Phantom 4 drone can achieve a GSD of at least 0.7 centimeters per pixel with just its built-in camera. For context, this spatial resolution would use approximately eighty-five pixels to display an average human eye, and facial recognition software only needs about three pixels per eye to operate effectively. Because drones can offer a spatial resolution at least 2000 times greater than most publicly available satellite imagery, the potential privacy impact of drone-captured images greatly exceeds that of satellites.

Both Google Earth and Bing Maps supplement satellite imagery with aerial imagery from manned aircraft. Bing’s Bird’s Eye offers aerial photographs of people’s homes taken at a 45-degree angle of view from an altitude of 1000 feet. “This Bird’s Eye imagery is


204. Seifert et al., supra note 193, at 1256–57.

205. This calculation was made by using the dimensions of the human eye to calculate the surface area of an ellipse (oval). Inessa Bekerman, Paul Gottlieb & Michael Vaiman, Variation in Eyeball Diameter of the Healthy Adult, J. OPHTHALMOLOGY (2014), https://www.hindawi.com/journals/joph/2014/503645/ [https://perma.cc/56SQ-F9U6] (“The size of a human adult eye is approximately 24.2 mm (transverse[ ]) × 23.7 mm (sagittal[ ]) × 22.0–24.8 mm (axial) with no significant difference between sexes and age groups.”). Because the sagittal plane is used to measure the depth of a human being in body imaging, the other two measurements are relevant to determining the area of the human eye. Basic Plane Mathematics of MRI, My-MS.ORG, https://my-ms.org/mri_planes.htm [https://perma.cc/ZN9M-UHLZ]. These dimensions provide the necessary figures to calculate the area of an ellipse. Area of an Ellipse Calculator, KEISAN ONLINE CALCULATOR, https://keisan.casio.com/exec/system/1223289167 [https://perma.cc/JQX7-6DKZ] (using 24.2 for a and 23.4 for b). The result is approximately 1779 square millimeters of area for the eye at its largest cross section. Because the visible area of the eye is smaller than this cross section and is partially covered by eye lids, let us assume that under normal circumstances the visible area of the eye has one-third the area of this largest possible ellipse. The visible area of the eye therefore has an area of about 593 square millimeters. Dividing 0.7 centimeters (7 millimeters) of spatial resolution, see supra note 189, into 593 square millimeters equals 84.7 pixels.


sub-10 CM [centimeter] GSD (ground sample distance), which . . . support[s] more detailed levels of map zoom.” For a fee, Bing’s worldwide coverage is limited to spatial resolution of thirty centimeters per pixel. Google Imagery, also a fee-based service, offers up to fifteen centimeters per pixel spatial resolution. Accordingly, drones can offer a spatial resolution at least fourteen times greater than publicly available aerial photography.

Temporal resolution offers a strong distinction between images captured by drones and those captured from aerial photographs and satellite images. Drones can capture images at least daily if not more frequently, making their temporal resolution instantaneous with live streaming during the course of a single flight and just hours in between battery charges. The Landsat 8 satellite has a temporal resolution of sixteen days, but Google and Bing do not update their images that frequently. Publicly available aerial images are captured at irregular intervals. Though not a form of remote sensing because the camera platform is on the ground at the moment of image capture, the “street views” offered by Google Maps and Bing Maps display images taken once every few years. These significant differences in temporal resolution make the images captured by drones fundamentally different from other publicly available aerial and satellite images.

K6. Because Bing’s Bird’s Eye focuses on images of populated areas, the minimum safe altitude for flight operations is 1000 feet. 14 C.F.R. § 91.119(b) (2020).
208. Bing Blogs, supra note 207.
211. Services like EagleView, see supra notes 138–39 and accompanying text, may offer the possibility of aerial photography with greater spatial resolutions. Such images, though, would likely only be captured with specific instructions from the customer. Unless the images are of property in which the customer has a legal interest, there may be other protections deterring such image capture of strangers’ homes. See, e.g., infra note 382.
212. Gonzalez, supra note 34, at 295.
213. See supra notes 117–18 and accompanying text.
214. Landsat 8, supra note 203.
215. See Lesiv et al., supra note 201, at 3–5.
216. See id.
Publicly available images of the author’s home help illustrate the extent of these differences. The street view images of his home were captured several years before he moved in. The nadir satellite imagery is several years old because of changes in vegetation. Though Bing’s Bird’s Eye imagery has a spatial resolution with approximately 4-centimeter GSD, these images of his home were captured sometime in the spring of 2019. The Google Earth 3D imagery features a tree that is no longer in the yard. When a drone captures an image, the spatial and temporal resolution are consistent. Drone image capture, accordingly, is a vastly more accurate representation of someone’s home than publicly available satellite and aerial photographs. The difference in the representativeness of the image is akin to the distinction between an impressionist-style painting and a polaroid photograph inscribed with the date the picture was taken.

C. **Distinguishing Drones from Neighbors’ Elevated Vantage Points**

All these distinctions among images captured from drones, manned aircraft, and satellites can be summarized as follows: drones can operate at angles and in proximities to the objects captured in images that are unavailable to other image capture technologies. When considering the privacy of the home, only a neighbor’s elevated vantage points—windows, balconies, roofs, treehouses—offer a similar field of view and proximity. Drones can operate in this same airspace. Before continuing the discussion, it is important to define some key terms.

The person in question is the *occupant*. This term includes all parties who are on property lawfully, regardless of the scope of their authority to be there. The totality of the property is called the *home*. This includes the structure in which the occupant has the greatest refuge from public observations—the *dwelling*.

---

218. *See* Lesiv et al., *supra* note 201, at 118 (publicly available images from satellites).
219. *See infra* Part IV.
221. *See* Francis C. Amendola et al., *Annotation, House; Home; Home Place; Building; Dwelling; Homestead; and Similar Terms*, 96 C.J.S. Wills § 1263 (Dec. 2020).
222. *Id.*
part of the home, the area immediately around the dwelling is called the \textit{curtilage}.\footnote{See Oliver v. United States, 466 U.S. 170, 180 (1984).}

A neighbor can be understood as the minimum definition of the public—the single someone that is not an occupant of the home but can observe at least part of the dwelling or curtilage shielded from the view of all others.\footnote{See Bruce G. Brener, \textit{The Supreme Court and the Fall of the Fourth Amendment}, 25 \textit{Val. U. L. Rev.} 383, 388–92 (1991) (discussing cases of observations from neighbor’s windows where no Fourth Amendment search was found); Stuart P. Green, \textit{To See and Be Seen: Reconstructing the Law of Voyeurism and Exhibition}, 55 \textit{Am. Crim. L. Rev.} 203, 209–11 (2018) (distinguishing mere observations or displays through a home’s windows from criminal acts of voyeurism and exhibition, respectively, based on the observer’s or occupant’s illegal intent). By considering a neighbor “the public,” the police can adopt the neighbor’s vantage point to conduct a variety of warrantless searches. See, e.g., Gregory E. Sopkin, \textit{The Police Have Become Our Nosy Neighbors: Florida v. Riley and Other Supreme Court Deviations from Katz}, 62 \textit{U. Colo. L. Rev.} 407, 407 (1991).} The field of view from a neighbor’s elevated vantage points may offer a look directly into the dwelling or curtilage unavailable from ground level, manned aircraft, or satellites. From these places, privacy fences offer little visual obstruction and second-story rooms can be observed at the neighbor’s eye level.

Such observations posts are permanent, or at least very slow to change. In addressing the question, “can the neighbor see into the occupant’s home,” there is a balance of information.\footnote{See Xiaodong Jiang, Jason I. Horye \& James A. Landay, \textit{Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing}, UbiComp 2002, Sept. 2002, at 176–77.} With a quick glance from her curtilage or out her bedroom window, the occupant can see her neighbor’s windows, roof, balconies, even treehouses. If someone is there, then the occupant knows the neighbor can observe her in that moment. If someone is not there, the occupant is free from the neighbor’s visual observations.

The occupant’s tolerance for visual observation from the neighbor will dictate her response to this information. Seeking to assure privacy for a moment, the occupant might block her windows by drawing the curtains.\footnote{Id. at 181 (“[S]ocial norms have evolved to the extent that most people would . . . shield their windows.”).} Because the neighbor’s elevated vantage points are fixed, an occupant has all the information she needs to erect permanent barriers that preserve her desired level of privacy. Awnings and frosted glass offer a more permanent solution for the
home.\textsuperscript{227} To create private spaces in a curtilage already surrounded by a privacy fence an occupant might strategically plant trees,\textsuperscript{228} erect a taller fence,\textsuperscript{229} or build a roof over part of the curtilage.\textsuperscript{230}

Drones present significant \textit{information asymmetries}.\textsuperscript{231} Particularly when compared to a neighbor’s fixed vantage points, drones’ maneuverability and responsiveness to operator intent mean that they can move freely through the air.\textsuperscript{232} The drone operator has access to countless fields of view whenever she elects to fly. The occupant now has no information about which field of view the drone is using at any point in time. The precisely affixed awning, the strategically planted tree, and the carefully constructed roofed patio now offer no privacy protection.\textsuperscript{233}

A drone’s undetectability compounds these information asymmetries.\textsuperscript{234} The information signals offered by the neighbor’s fixed vantage points all but disappear. A quick glance out the window or over the fence conveys all the information an occupant needs about whether the neighbors can observe each other. If the neighbor’s curtains are closed, the occupant is assured of freedom from observation even if her window treatments remain open, and vice versa. Though there may be periods of time when both sets of window treatments are open, an occupant needs only periodic glances out at the neighbor’s fixed vantage points to determine if the neighbor can see into the dwelling. Because of their size, low noise profile, and unpredictable flight patterns, drones are very difficult to detect.\textsuperscript{235} Short of constantly peering out the window or scanning the sky in multiple directions while outside, only keeping window

\begin{itemize}
\item \textsuperscript{227} The British have codified such architectural features as necessary elements for assuring freedom from a neighbor’s visual observations. See Mike Dade, \textit{Planning: Solutions to Overlooking Issues}, \textit{BUILD IT} (Sept. 6, 2020), https://www.self-build.co.uk/planning-overlooking/ [https://perma.cc/U5SH-LTPQ]; see also Privacy Lost Through Neighbours New Window, BERGAGUE ABOGADOS (Feb. 28, 2018), https://www.berdaguerabogados.com/neighbour-privacy/ [https://perma.cc/9BEQ-NCQE].
\item \textsuperscript{228} Florida v. Riley, 488 U.S. 445, 448 (1989) (“[T]he contents of the greenhouse were obscured from view from surrounding property by trees . . . .”).
\item \textsuperscript{229} California v. Ciraolo, 476 U.S. 207, 209 (1986) (describing the presence of a second, taller privacy fence that blocked neighbors’ views of the curtilage).
\item \textsuperscript{231} Friedman, \textit{supra} note 43, at 11.
\item \textsuperscript{232} See \textit{supra} sections III.A.2, III.A.4.
\item \textsuperscript{233} Friedman, \textit{supra} note 43, at 14–15.
\item \textsuperscript{234} See \textit{supra} section III.A.5.
\item \textsuperscript{235} Id.
\end{itemize}
treatments drawn or staying indoors can ensure the occupant of freedom from unwanted visual observation.

To put it differently, no temporary solutions ensure freedom from unwanted visual observations made by drones. These information asymmetries leave the occupant with a difficult choice: forego her desired level of privacy or sacrifice her enjoyment of her property by erecting “drone-proof” barriers to visual observation. This is the exact choice that Justice Brennan warned of in his dissent in the helicopter overflight case, Florida v. Riley.236 “The question is not whether you or I must draw the blinds... It is whether you and I must discipline ourselves to draw the blinds every time we enter a room, under pain of surveillance if we do not.”237 Because this question arose as a dissent in the context of observations made via a helicopter, the issue is not unique to drones. Rather, Justice Brennan simply pointed out a problem in U.S. privacy jurisprudence that drones highlight almost perfectly.

A neighbor’s fixed vantage points do not create the same issues. For this reason, drones can be distinguished from a neighbor’s fixed vantage points.

By distinguishing drones from other aircraft, image capture technologies, and a neighbor’s fixed vantage points of visual observation, it is now possible to explain precisely how drones have a unique impact on unwanted visual observations in and about the home.

---

IV. DEFINING PRIVACY IN THE HOME—FREEDOM FROM VISUAL OBSERVATION & THE DRONE DATA LIFECYCLE

For the purposes of this discussion, “privacy” means freedom from visual observation in and about the home. After an introduction of key terms, this Part organizes non-drone-specific privacy protections spatially. Starting from the physical spaces inside the home which have the greatest legal protections from being observed, the discussion moves physically outward to spaces with fewer protections. The legal protections described here may be actionable in factual scenarios involving drones, but successful actions involving drones under these theories present significant challenges.

The legal protections discussed here focus on drone operations by private actors. Government actors, though, might direct private drone operators or, at a later time, use the images captured by private drone operators. A full picture of the protections against private actors operating drones, therefore, must include the government use of drones as well.

This definition of privacy strongly implicates two conceptions of privacy: surveillance and secrecy; as well as two legal theories of privacy: reasonable expectations and property rights. The legal protections for privacy in each of these spaces are discussed within the conceptual and theoretical frameworks. Building on this, a discussion of privacy expectations in drone data concludes the Part.

---

238. See supra Part I.
240. See supra notes 25–28 and accompanying text.
241. See, e.g., Office of the Attorney Gen., U.S. Dep’t of Justice, Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems 11 (Apr. 13, 2020) (“Department components may maintain records of communications to or from unmanned aircraft or unmanned aircraft systems intercepted or acquired under authority of the Act . . . .”).
A. **Key Terms**

The terms *occupant*, *home*, *dwelling*, and *curtilage* are defined above. Anywhere beyond the scope of the curtilage is called *open fields*. The concept of *trespass* most applicable to drones is trespass quare clausum fregit. This definition of trespass recognizes a “direct causal relation between the conduct of the actor and the intrusion of the foreign matter upon the possessor's land . . . sufficient to create a trespass.”

B. **A Spatial Tour of Privacy Interests in the Home**

1. **Parts of the Interior of the Dwelling Not Visible to the Public**

The parts of the interior of the dwelling that are not visible to the public enjoy the highest level of privacy protections. A drone would have either to trespass into the dwelling or use extra sensory (beyond the visible light spectrum) remote-sensing technologies to make a visual observation of these spaces. Under either set of circumstances, the occupant of the home could pursue recourse against a private drone operator under criminal statutes, civil trespass, and possibly even the privacy torts of intrusion upon seclusion and publicity given to private life. A government actor using a drone would need a warrant both to enter these spaces and to use extra sensory technology to make a visual observation of these portions of the dwelling not otherwise visible to the public view.

Depending on the features of one’s dwelling, drones may be able to make visual observations of places not otherwise visible to the public. A low window might sit under an awning and behind a privacy fence. It offers no view of public spaces. This window is not

---

242. See supra notes 220–23 and accompanying text.
245. Restatement (Second) of Torts ch. 7, topic 2, scope note (Am. Law Inst. 1965).
247. Restatement (Second) of Torts § 158 (Am. Law Inst. 1965).
visible to the public, not even the neighbor on the other side of the privacy fence. With a drone, though, the neighbor could achieve a field of view into the window by flying on her own property over the height of the privacy fence but under the height of the awning. If low overflight via drone does not constitute trespass, the neighbor may be able to access additional fields of view from the occupant’s curtilage. A drone, therefore, presents a unique means of making unwanted visual observations of interior spaces of a dwelling not otherwise visible to the public.

2. Parts of the Interior of the Dwelling Possibly Visible to the Public

The next highest level of privacy protections covers places like bedrooms and bathrooms. These places are recognized as especially private, even if they are potentially capable of visual observation from a public vantage point. A bedroom window may overlook a neighbor’s window, thereby allowing for the possibility of visual observations by drone from a public vantage point. Even if the occupant does not specifically prevent visual observations from the public, society recognizes that these places enjoy a heightened level of privacy protection because occupants are likely to be nude or intimate in such places.

Privacy interests may be protected from private actors by voyeurism statutes and potentially even the privacy torts, even if the drone is flying in a public space. In some states, though, the question of whether the occupant attempted to prevent visual observations of these particularly private spaces (i.e., by closing the curtains) may be relevant. If the spaces in the dwelling capable of visual observations from a public vantage point are not generally

252. See Scharf, supra note 23, at 1089 n.185 and accompanying text.
253. See id.
254. See, e.g., Wash. Rev. Code § 9A.44.115; Okla. Stat. tit. 21, § 1171. In this Article the term “voyeurism statutes” is used to refer to the class of laws that makes it a criminal offense to make visual observations of others. This includes the crimes of voyeurism, surveillance, peeping Tom, and invasion of privacy. Regardless of how the crime is named, a necessary element of each of these crimes includes making unwanted visual observations.
considered especially private, like a kitchen or a second-story TV room, then the occupant’s efforts to shield the space from view determines the availability of privacy protections from unwanted civilian observers.257

In other words, if the blinds are down privacy protections exist, but if they are open the same privacy protections from private actors are not available.258 The occupant’s privacy expectations in these spaces are irrelevant to the question of a government actor’s visual observations from a public vantage point.259 For government actors making visual observations from a public vantage point the most relevant question is whether the interior of the dwelling is in “plain view.”260

Drones also have a unique impact on privacy in spaces possibly visible to the public. A quick look out an open window, and the occupant knows if the neighbor’s blinds are open or if the neighbor is on her balcony. She can shield the interior of her dwelling from public view by closing her own curtains. Especially when compared to a neighbor’s fixed vantage points, drones are nearly undetectable.261 The occupant would have to see or hear a drone in flight to know that it is making observations.262 Without this piece of information, the occupant might not close her curtains. Accordingly, she would enjoy fewer legal protections from unwanted visual observations made via drone.

The informational asymmetries presented by drones, therefore, have a unique impact on privacy in parts of the dwelling possibly visible to the public. But, because this exact issue arose over thirty years ago relative to helicopter operations,263 it is difficult to argue that drones present a novel threat to privacy. Rather, drones simply highlight a preexisting issue in U.S. privacy jurisprudence.

258. See, e.g., 9 Guam Code Ann. § 70.35(d)(10).
261. See supra section III.B.5.
262. See supra section III.C.
263. See supra notes 228–29 and accompanying text.
3. Portions of the Curtilage Not Visible from the Ground and Not Visible the Air

Moving to the outside of the dwelling, the portions of the curtilage not visible both from the ground and not visible from the air receive the next highest level of privacy protection. These spaces might be understood as roofed structures within a yard that is surrounded by a privacy fence. Such structures might include sun porches, covered patios, pergolas, gazebos, and foliage covered trellises. The space underneath the roof of the structure is not visible to observations made from a public space either on the ground or from overhead positions. Under these structures an occupant seeks to enjoy a semi-open space within the curtilage but has taken clear measures to assert a privacy interest both from the ground, and elevated positions, including the air. From the ground, the privacy fence necessitates trespass to make visual observations.

In the overflight cases of homes—Ciraolo and Riley—the Supreme Court reasoned that manned airways, as low as 400 feet in altitude, constitute a public vantage point. Though drones fly at lower altitudes, they could operate in such a way that their fields of view are similar to those of manned aircraft, then visual observations from above are rendered nearly impossible because of the roof-like cover over these structures. If constructed properly, the space underneath these structures may not even be visible from elevated fixed vantage points on a neighbor’s property.

A drone could operate at such a height and location relative to the ground that its camera has a field of view that is higher than the fence but lower than the elevation of the roof of the structure in question. See Figure 2 below. If the drone crosses over the property line in question to achieve this field of view, that may constitute trespass. If a drone operates from a public (nonprivate) vantage point, then only certain voyeurism statutes and the privacy

267. See supra sections III.A, III.B.2.
268. See Riley, 488 U.S. at 447 (holding that visual observations from the air did not constitute Fourth Amendment search because a structure in the curtilage was partially uncovered).
270. See, e.g., VT. STAT. ANN. tit. 13, § 2605.
torts would potentially offer protection from unwanted visual observations by private actors. The specific factual circumstances would dictate whether the Fourth Amendment would provide privacy protection from such visual observations by a government actor. Absent circumstances that would trigger any of these protections, though, drones have a unique impact on privacy because they offer a field of view of the curtilage unavailable by other means.

Figure 2—Drone-Captured Image of Back Yard with Privacy Fence and Covered Porch

This set of circumstances provides the most support for assertions by others that drones have significantly impacted privacy,

272. See United States v. Jones, 565 U.S. 400, 413–14 (2012) (Sotomayor, J., concurring); see also Blitz et al., supra note 24, at 140.
particularly from warrantless observations by government actors.274 By placing a roofed but unwalled structured behind a privacy fence, an occupant can largely be free from visual observations from manned aircraft. If an occupant wants to avoid visual observations from drones in parts of her curtilage, *Ciraolo* and *Riley* could effectively require that such spaces be moved indoors—covered with roofs and walls that obscure all possible visual observations because drones can lawfully achieve almost any field of view. The occupant must choose between enjoyment of her curtilage as an outdoor space and freedom from visual observation.275 Drones, therefore, have a unique impact on privacy under these circumstances.

These circumstances, though, are not very common. Drones with a field of view over privacy fences but under the roofs of unwalled structures might catch a glimpse of a patio set, an outdoor kitchen, or winter vegetables in a high tunnel. Except for outdoor hot tubs, these are not spaces where people tend to expect much more privacy than what is already achieved by erecting a privacy fence. People build these roofed but unwalled structures to enjoy some shade in their back yard. The net effect in the application of the privacy torts and voyeurism statutes, therefore, is minimal. Accordingly, though drones have a unique impact on privacy under these circumstances, claims that drones can have a *significant* impact on privacy simply lack factual support.

4. Portions of the Curtilage Possibly Visible to the Public

If located inside a privacy fence, roofed but windowed outbuildings such as garages, sheds, and treehouses enjoy a lower level of privacy protections. Making observations from the ground, it would be difficult to see inside the windows of such structures. Like with other roofed structures inside the privacy fence,276 the location of a drone making the visual observation would determine whether the occupant can use trespass as a recourse against such observations. If a government actor trespasses to make these observations, it is likely that the occupant could assert Fourth

274. *See supra* notes 3–4; Spelman, *supra* note 60, at 402.
276. *See supra* section IV.B.3.
Amendment protections. Trespassory observations by private actors could also be actionable.

However, the occupant likely has a diminished expectation of privacy in these types of structures, particularly from visual observations by government actors.277 If either a government actor or a private party makes visual observations without trespass, it would be difficult to assert any privacy protections. Because of a diminished expectation of privacy in such places, the occupant’s successful use of voyeurism laws or the privacy torts would rely on a very particular set of circumstances.

Treehouses, though, present an interesting case regarding freedom from visual observation. Due to a treehouse’s elevation, a public vantage point at ground level would offer a limited field of view of the interior of the treehouse. A public vantage point of a similar height, like a neighbor’s second-story window, might offer a public view into the treehouse. Assuming there is no public vantage point from a similar height, then the interior of the treehouse would effectively be private. Visual observations would likely necessitate trespass.

A drone, though, could easily achieve the necessary altitude and observe the interior of the treehouse without trespassing. Despite diminished privacy expectations in it generally, a treehouse is considered a “child’s playhouse . . . built in a tree.”278 Children are sometimes afforded greater privacy protections than adults.279 Accordingly, unwanted visual observations of children in treehouses made by drone may be actionable against private actors.280 In the absence of another public vantage point, therefore, a drone could have a unique impact on a child’s privacy in a treehouse.

280. E.g., LA. STAT. ANN. § 14:283(B)(4).
5. Portions of the Curtilage Not Visible from the Ground or Not Visible from the Air, but Not Both; Open Fields

The areas shielded from ground level visual observations from a public location enjoy a very low level of privacy protection. A privacy fence could evince the occupant’s desire to be free from ground level visual observations around a back yard, for example. Visually observing such spaces from the ground would likely necessitate trespass. But, making visual observations of such spaces from the air would not constitute a trespass.281 Relative to the operations of a drone, therefore, visual observations could be made from some public vantage point that would not require trespass, and therefore would not limit a government actor. Because some public vantage point of these spaces would always be available, it would require a fact-intensive analysis to determine whether the occupant had enough of an expectation of privacy to find recourse against private actors under the voyeurism statutes or privacy torts.282

Similarly, areas shielded from aerial observation but not ground level observation probably enjoy no privacy protections. For such structures, like car ports or porches covered with an awning, the occupant would only be able to assert a privacy interest against aerial observations. Visual observations from public vantage points on the ground would always be available. The occupant, therefore, likely has no recourse against either government actors or private actors making visual observations of these spaces.283

For spaces visible from either the ground or the air, but not both, an occupant enjoys little legal protections from visual observations. Beyond the curtilage, if a home is large enough, a home’s open fields also have no protections from unwanted visual observations by government actors.284 Trespass actions, though, may be brought against private actors.285 In all these spaces, drones offer no unique impact on privacy.

282. See Dolan & Thompson, supra note 255, at 20–21.
283. See Villasenor, supra note 11, at 502–03.
285. See infra section V.B.1.
6. Other Protections from Visual Observations

If an occupant has erected a privacy fence, the system of zoning rules and housing covenants also offers an occupant some protection from unwanted visual observations of the home. As Troy Rule has observed, “Height restrictions in zoning ordinances and private subdivision covenants further strengthen landowners’ certainty about their degree of privacy on their parcels by restricting neighbors’ ability to erect structures that could create new vantage points for peering over trees or fences.”286

On a case-by-case basis, the occupant could also acquire a light and air easement from a neighboring property. This would grant the occupant an interest in the unobstructed “passage of light and air over the property of another.”287 In combination with a privacy fence, such an easement would prevent the neighbor from building structures that offer a vantage point for visual observations of the occupant’s home. These protections for visual observation, though, are not unique to drones.

Additionally, if another’s drone use bothers the occupant such that it diminishes her enjoyment and use of her home, the occupant may be able to bring a private nuisance claim.288 Among the elements the occupant would typically have to prove for a successful private nuisance claim, the drone use would have to be repeated (not just a single incident) and the manner of operation of the drone would have to be generally considered offensive.289 Offensive behavior via drone may include capturing images of parts of the home that are generally considered private, thereby causing unreasonable injury.290 A successful private nuisance claim would be difficult,291 but could prevent future visual observations of the occupant’s home. Private nuisance actions, though, are not unique to drones.

286. Rule, supra note 239, at 189.
287. 6 MILLER & STARR CAL. REAL EST. § 17:35 (4th ed. 2015).
289. Id. §§ 821D, F.
290. Wood v. Picillo, 443 A.2d 1244, 1247 (R.I. 1982); see Farber, supra note 73, at 395.
291. See Farber, supra note 73, at 395.
A negative drone avigation easement—called here a “Teddy Easement”\(^{292}\)—could limit the occupants of nearby properties from making visual observations from the air space over their respective properties. Avigation easements typically authorize manned aircraft to fly at otherwise trespassory altitudes, particularly in take-off and landing zones of airports.\(^{293}\) A Teddy Easement could prevent drones from flying over the burdened properties, thereby stopping drones from accessing otherwise public vantage points that allow visual observations of the easement holder’s (beneficiary’s) home. A Teddy Easement would be a legal protection unique to drones. The author, however, has not found any instance of such an easement burdening a property.

7. Shifting Focus from Operations to Data Gathering

Drones potentially have a unique impact on privacy in four spaces in and around the home: (1) parts of the interior of the dwelling not otherwise visible to the public; (2) parts of the interior of the dwelling possibly visible to the public; (3) portions of the curtilage not visible from the ground and not visible from the air; and (4) in the absence of another public vantage point, treehouses used by children. These spaces represent a rather limited set of factual circumstances. Accordingly, assertions that the unique operating capabilities of drones have a significant impact on privacy simply lack factual support.

\(^{292}\) This legal solution was inspired by the author’s dog—Teddy. Though there are no trees or structures in the author’s yard where one might find a squirrel, the neighboring yards have several tall trees, utility poles, and power lines. Squirrels run amok in the neighbors’ trees and across their power lines. Upon sensing them, Teddy prowls the author’s fence, running, whining, and barking at all hours. The author has had no success explaining to Teddy that the squirrels are not on his property and he has no chance of catching them. The author often wonders, “how can I stop the squirrels?,” for Teddy is a perfect dog and does not need to change in any way. If only there were an anti-squirrel easement! Teddy and the squirrels bear a striking resemblance to drones making visual observations of an occupant’s home. From this perspective, the occupant should not need to change anything about her home. Rather, how could she ensure that drones do not operate over neighboring properties such that they could make unwanted visual observations of her home?

Drones, though, are primarily data collection devices. Whether the captured image is unique to drones’ operating abilities or not, the privacy impact of drones must consider the lifecycle of drone-captured data. A discussion about conceptions and theories of privacy helps explain the extent to which these legal approaches protect the home from unwanted visual observations from drones. With this understanding, the impact of drone data on the third-party doctrine can be better understood.

C. Conceptions and Theories of Privacy

This discussion of conceptions and theories of privacy seeks to explain the reasoning behind the protections from unwanted visual observations an occupant enjoys in and around the home. These conceptions and theories may be articulated through Fourth Amendment jurisprudence, but they are important to understanding protections against drone operations by private actors. Occupants seeking to protect themselves from drones making unwanted visual observations in the home cannot discriminate between the private drone operators and government drone operators. Additionally, government actors may commandeer private drone operators or, at a later time, use the images captured by civilian drone operations. Accordingly, though the reasoning behind these privacy protections may be articulated in the context of visual observations by government actors, this reasoning also applies to the protections against private actors.

1. Property Theory of Privacy

One legal theory of privacy interests comes from the realm of property. Property rights serve to protect one’s privacy interests mainly by physically excluding others. Violation of this exclusion is considered trespass. If someone trespasses into the occupant’s

---

294. See supra notes 70–73 and accompanying text.
295. See supra notes 25–28 and accompanying text; see also California v. Cirado, 476 U.S. 207, 209 (1986) (discussing the police use of a private aircraft to make visual observations); Florida v. Riley, 488 U.S. 445, 448, 450–51 (1989) (arguing that observations by a government helicopter in public airspace did not constitute a search because privately operated helicopters could also fly there).
296. See supra note 241 and accompanying text.
home, then the property theory of privacy would serve only indirectly to prevent visual observations. Accordingly, the Supreme Court has found that privacy interests may be violated when the government conducts searches that effectively require physical intrusion upon private spaces. The property theory of privacy, therefore, does not protect against visual observations of the home from public (nonprivate) vantage points.

The property theory of privacy offers the basis for privacy protections achieved through zoning laws, negative drone avigation easements, and the private nuisance cause of action. Absent these specific circumstances, the steps an occupant takes to prevent visual observations from the public become important. If someone is in a public space and she happens to make a visual observation of the interior of a home, then it is not clear that the occupant has legal recourse against those making such visual observations. Observations of spaces shielded from public view become impossible without effectively committing trespass. The property theory, therefore, helps explain the legal protections only for parts of the interior of the dwelling not visible to the public except by trespass. Via drone, observations of all other parts of the home might be made without trespass. It is not clear, therefore, that the property theory supports protections against unwanted visual observations in any other area of the home.

2. Privacy as Surveillance

If privacy is understood as freedom from unwanted visual observation in and about the home, this strongly implicates the conception of privacy as surveillance. Surveillance can be understood as the collection of information about a person or place.
lance focuses on the actions of the observer, not necessarily the inter-

302 Surveillance may be indiscriminate or specifically targeted at the home or occupant in ques-

303 If the home is subject to surveillance by drone it means that the occupant’s privacy interest is impinged at the moment of image capture. 304

Like the property theory of privacy, surveillance helps explain trespass as a privacy protection. Accordingly, surveillance fully supports privacy protections only for parts of the interior of the dwelling not visible to the public. Except for voyeurism statutes with specific intent requirements that eliminate the occupant’s burden to block all visual observation from public spaces, 305 surveillance only helps explain legal protections of other areas of the home to the extent that the occupant has shielded those spaces from public view. If visual observation via drone is possible from a public vantage point, the surveillance conception of privacy offers almost no protection from unwanted visual observations in and around the home.

3. Reasonable Expectations Theory of Privacy 306

The concurring opinion by Justice Harlan in Katz v. United States articulated the reasonable expectations theory of privacy. 307 Harlan articulated a test: “[t]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of

302 See Christopher Slobogin, Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards, 10 HARV. J.L. & TECH. 383, 431–32 (1997) (discussing the merits of various surveillance techniques based on the extent to which the observer intrudes upon the observed, not the privacy expectations of the observed).

303 Villasenor, supra note 11, at 501–03.

304 See id. at 494.

305 See, e.g., OHIO REV. CODE ANN. § 2907.08 (LexisNexis 2009); see also supra note 254 and accompanying text.

306 Both the reasonable expectations and property theories of privacy interests have been hotly debated by the Court and scholars. See United States v. Jones, 565 U.S. 400 (2012); Carpenter v. United States, 138 S. Ct. 2206, 2244 n.10 (2018). Though the Court in Jones seems to have moved away from the reasonable expectations theory, it is not clear that this basis for privacy protections has been completely abandoned. 565 U.S. at 415 (Sotomayor, J., concurring); Jeramie D. Scott, Drone Surveillance: The FAA’s Obligation to Respond to the Privacy Risks, 44 FORDHAM URB. L.J. 767, 784–85 (2017).

privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” In applying the Harlan test to freedom from visual observation in the home, the first question is whether the occupant has subjectively demonstrated an expectation of privacy. In the case of visual observations made by drones, this subjective demonstration must be tangible. Privacy fences, closed window treatments, and roofed outdoor spaces all serve to indicate that the occupant expects to be free from visual observation in and around her dwelling. Society has generally considered the home the most private of spaces. Expectations of freedom from observation in and around the home, therefore, are reasonable.

When the occupant has erected barriers to visual observation from public vantage points, the reasonable expectations theory also helps explain trespass as a privacy protection. Unlike with the property theory and the surveillance conceptions, an occupant establishes her expectation of privacy simply by erecting some barrier. It is not necessary to shield all possible public views. This eliminates the need for an observer to trespass to justify recourse against unwanted visual observations. An occupant, therefore, may use many of the voyeurism statutes as well as the privacy torts to advocate her privacy interests. For spaces that are possibly visible from the public, either in the dwelling or in the curtilage, the reasonable expectations theory explains why privacy protections against visual observations made by drones operating in public spaces could still be used.

4. Privacy as Secrecy

The *secrecy* conception of privacy focuses on an individual’s ability to keep from disclosure information about herself. Unlike surveillance, secrecy focuses on the expectations of the observed,

---

310. *See*, e.g., WASH. REV. CODE § 9A.44.115(2)(a)(ii).
not the actions of the observer. And unlike the reasonable expectations theory of privacy, an occupant does not even necessarily need to erect barriers specifically to prevent visual observations. For example, portions of someone’s body not typically exposed to the public may constitute private information about a person. Or, information about a child may be considered de facto private information. If an adult is in her bedroom or bathroom but the curtains are open, secrecy helps explain why she may still have recourse against a drone operator making unwanted visual observations under some voyeurism statutes. Privacy interests may be advocated through the privacy torts even if visual observations of places other than the bedroom or bathroom, such as the fenced-in backyard, are possible from a public vantage point. Protections from unwanted visual observations of children can also be explained by this conception of privacy.

D. Third-Party Doctrine and Drone Data Flows

These theoretical and conceptual understandings of legal protections offered against unwanted visual observations made by drones help explain the legal status of drone data. As discussed above, drones are primarily data collection devices. The data in question, for the purposes of this Article, are images of the home and its occupants. Drone software programs nearly automatically share drone images with the drone software provider. Once in the hands of the drone software provider, the images are considered both shared and a business record.

From the perspective of an occupant’s privacy interests, business records fall under the third-party doctrine. Though it has taken several forms in Supreme Court jurisprudence, the third-party doctrine maintains that one cannot assert a privacy interest over

---

313. See, e.g., GA. CODE. ANN. § 16-11-91(b)(1).
315. See supra notes 70–73 and accompanying text.
316. See supra section IV.B.
317. See supra note 17.
318. See Aldrich, supra note 18, at 5.
319. See Blitz et al., supra note 24, at 65 n.76.
something that has been knowingly shared with a third party.\textsuperscript{320} Without a privacy interest in the drone-captured images, the occupant cannot seek Fourth Amendment protections against government use of the images and is less likely to be successful in private causes of action. The default state of many drone software programs is to store drone-captured images remotely,\textsuperscript{321} and the drone software provider even potentially sells it.\textsuperscript{322} The different conceptions and legal theories of privacy illustrate the challenges the third-party doctrine presents to an occupant asserting a privacy interest in drone-captured data.

As discussed, the property theory of privacy only protects against visual observations by drone to the extent that drone operations involve trespass.\textsuperscript{323} The occupant has no privacy interest in the drone-captured images taken from a public vantage point. Considering that drones can access countless fields of view without committing trespass, an occupant must keep her blinds closed and build walls and roofs over all parts of her curtilage she intends to keep private.\textsuperscript{324} Drones did not create this difficult choice, rather they simply take the reasoning behind a trespass-based privacy jurisprudence to its logical extreme. From the perspective of the third-party doctrine, the occupant has no privacy interest in any drone-captured images of any part of her property captured without trespass. The third-party doctrine prevents her from stopping the drone software provider from keeping, sharing, or selling such images of her home.

The surveillance conception indicates that privacy interests are diminished at the moment of image capture.\textsuperscript{325} The occupant of a home, therefore, would effectively have to make her home impenetrable to surveillance from a public vantage point to have a privacy

\textsuperscript{322} See Vacek, supra note 7, at 139; Scott, supra note 306, at 785–88; About, UNMANNED ROBOTICS SYS. ANALYSIS, https://ursasecure.com/about/ [https://perma.cc/9FU3-AACK] ("There is little regulatory or industry oversight or standards making process for the data generated by . . . [drones].").
\textsuperscript{323} See supra section IV.C.1.
\textsuperscript{324} See supra sections IV.B.2, IV.B.3; see also Spelman, supra note 60, at 402.
\textsuperscript{325} See supra section IV.C.2.
interest in drone-captured images. Like with the property theory perspective and the third-party doctrine, failure to erect such barriers prevents the occupant from asserting a privacy interest against the drone software provider’s use of the images.

The surveillance conception of privacy, though, can also help explain some of the specific intent voyeurism statutes. Accordingly, if someone captures an image from a public vantage point with voyeuristic intent, the occupant of the home may still have a privacy interest in those images. The occupant did not knowingly share those images with the voyeur. The drone software provider, therefore, should not have them in its possession. The occupant may be able assert a privacy interest in those images enough to avoid the application of the third-party doctrine.

Privacy protections supported by the reasonable expectations theory of privacy create a more nuanced question under the third-party doctrine. The issue turns on how one defines the knowledge standard within the third-party doctrine. What does it mean to know that drone-captured images have been shared with a third party?

From one perspective, knowledge might be established simply by the occupant having reason to know that a drone could possibly capture an image of some part of the home. By erecting barriers to visual observation, even if those barriers do not prevent all observations from a public vantage point, the occupant demonstrates a subjective privacy interest in preventing drone-captured images of her home. But by the very erection of those barriers the occupant signals that she knows that drone-image capture is possible. If she knows drone image capture is possible and she does not prevent it completely, then she has no reasonable expectation of privacy in the resulting images captured from a public vantage point.

This is the line of reasoning that the Court used in the manned aircraft observations of homes in Ciraolo and Riley. Both defendants erected some barriers to visual observation, but not complete barriers. The Court held that neither had a reasonable expectation of privacy. If this line of linking is applied to drones,

326. See supra section IV.C.2.
occupants must close their blinds and erect boxes impervious to visual observation across their curtilages in order to have a reasonable expectation of privacy. This choice arises not because the operational capabilities of drones, but because of this stringent standard that establishes a reasonable expectation of privacy. Without a reasonable expectation of privacy, an occupant would not be able to assert enough of a privacy interest to prevent a drone software provider from sharing images of the occupant’s home.

From another perspective, very specific information may be necessary to establish that an occupant knows that drone-image capture of her home is even possible. FAA rules for lawful drone operations require, among other things, that the operator keep the drone within her visual line of sight and only operate over people under certain circumstances. Additionally, some states and localities have laws that severely limit the possibility of lawful drone operations in residential areas. These rules may effectively prevent people from operating drones in populated neighborhoods. In fact, such rules have probably prevented the swarms of drones that many predicted would occupy U.S. skies. Granted, many have seen drones flying in public parks or at the beach, but lawful drone operations in residential neighborhoods is probably much less commonplace. Accordingly, it may be premature to assert that drone operations are ubiquitous. If drone operations in residential

329. See supra note 62 and accompanying text.
330. See supra note 66 and accompanying text.
331. See infra section VI.B.1.
332. E.g., Vacek, supra note 115, at 674; Farber, supra note 73, at 359; Schlag, supra note 3, at 11–12, 18–20.
333. The question of whether drones are truly ubiquitous for the purpose of privacy jurisprudence is still an open one and merits further analysis. Until the Operations Over People regulation takes full effect, it is not clear that flights over populated areas would be compliant with FAA regulations. See Operation of Small Unmanned Aircraft Systems Over People, 88 Fed. Reg. 4311, 4314 (Jan. 15, 2021). Additionally, applying Justice Scalia’s reasoning of proving the negative from Florida v. Riley, privacy expectations might still exist if drone flights over a populated area (e.g., someone’s home) “are unheard of.” Riley, 488 U.S. at 450–51. Applying the definition of privacy used in this Article, see supra Part I, privacy expectations are highest in populated locations because people’s homes are in such areas. Accordingly, if drones are not regularly flying above populated areas, then privacy expectations from unwanted visual observations via drone might still exist. There is strong evidence to suggest that drone operations are utterly absent from airspace above populated areas generally and will remain out of such airspace for years to come. See Joshua S. Turner, Katy J. Milner & Sara M. Baxenberg, FAA Adopts Final Rules for UAS Remote ID, Flights over People, and at Night, WILEY (Dec. 29, 2020), https://www.wiley.com/Alert-FAA-Adopts-Final-Rules-for-UAS-Remote-ID-Flights-over-People-and-at-Night [https://perma.cc/WK2L-RHCA] (noting that the UAS Traffic Management system (“UTM”) is necessary for the
neighborhoods are not ubiquitous, then it is reasonable for occupants to expect that their homes should be free from unwanted visual observations from drones. Absent direct evidence that a drone is operating near her home, an occupant may understandably not know that drones are capable of capturing images of her home.

If an occupant does not know that drones are operating nearby, then her reasonable expectations of privacy may be established by the erection of any barrier that prevents visual observation from both the ground and manned aerial vehicles. She does not know that drone-image capture is happening nearby. Her privacy inter-

deed use of drones and the absence of a network-based requirement from the final remote ID rule means that “UTM continues to be a long way off”); Simon Watkins, Jane Rosemary Burry, Abdulghani Mohamed & Matthew Marion, Ten Questions Concerning the Use of Drones in Urban Environments, 167 BUILDING & ENV’T 106458 (2020) (discussing the challenges to realizing the widespread use of drones); Drones and Coronavirus: Do These Applications Make Sense?, We ROBOTICS (Apr. 9, 2020), https://blog.robobtics.org/2020/04/09/drones-coronavirus-no-sense/ [https://perma.cc/4N6N-HKHS] (discussing that even in the emergent situation of the COVID-19 pandemic, it is difficult to deploy drones widely); Chris Gillis, Matternet Readies Cargo Drone for FAA Tests, FREIGHT WAVES (May 13, 2020), https://www.freightwaves.com/news/matternet-readies-cargo-drone-for-faa-tests [https://perma.cc/8AAY-HXPW] (“However, industry experts say the agency’s durability and reliability testing to certify airworthiness is rigorous. This will probably be measured in years rather than months, . . . . The strict safety requirements will require a lot of testing over a relatively long period of time.”); Brian Garrett-Glaser, Are Low-Altitude Weather Services Ready for Drones and Air Taxis?, AVIATION TODAY (Apr. 26, 2020), https://www.aviationtoday.com/2020/04/26/low-altitude-weather-services-ready-drones-air-taxis/ [https://perma.cc/REA6-SLUR] (discussing how inadequate low-altitude weather information may limit the widespread deployment of drones); Greg Nichols, The (Not-So-Secret Recipe) For a Commercial Drone Revolution, ZDNET (May 5, 2020, 10:00 AM), https://www.zdnet.com/article/the-secret-recipe-for-a-commercial-drone-revolution/ [https://perma.cc/NXDS-2W3G] (arguing that the lack of hardware and software standardization has prevented widespread drone proliferation); Thomas Kirschstein, Comparison of Energy Demands of Drone-Based and Ground-Based Parcel Delivery Services, 78 TRANSP. RES. PART D: TRANSP. & ENV’T 102209 (2020) (demonstrating that a widespread drone delivery system would consume more energy than a land-based delivery system).

Even when headlines suggest that drones are making deliveries in populated areas in certain communities, those flights appear to cover only a portion of the entire route, relying on drivers for the other portions of the delivery. E.g., Rafael Sánchez, Indianapolis Deli Makes Food Deliveries with a Drone, WRTV6 INDIANAPOLIS (Apr. 17, 2020, 9:09 AM), https://www.theyndychannel.com/open/indianapolis-deli-makes-food-deliveries-with-a-drone [https://perma.cc/TQG9-NJP3] (“Once the order is driven to a home or business, the drone operator who is FAA licensed drops off the food from several feet away.”); UPS Flight Forward, CVS to Use Drones to Deliver Medicines to Florida Retirement Community, AUVSI NEWS (Apr. 27, 2020), https://www.auvsi.org/industry-news/ups-flight-forward-cvs-use-drones-deliver-medicines-florida-retirement-community [https://perma.cc/R5EC-D5UL] (“During the first flights, which are expected to be less than one half mile, deliveries will be made to a location near the retirement community. To start, a ground vehicle will complete the delivery to the resident’s door.”).
est, therefore, is established even if the barriers do not prevent visual observation from all public vantage points accessible to drones. This line of reasoning supports successful applications of the privacy torts. From this perspective, an occupant would not know about the drone-captured images of her home held by the drone software provider. Therefore, the third-party doctrine would not be easily applied, and she could prevent the drone software provider’s use and sharing of the images.

An interesting question arises when an occupant actually knows that a neighbor owns and operates a drone. If the occupant does not erect barriers to prevent the neighbor’s drone from making visual observations, it could be difficult for the occupant to assert that she has a reasonable expectation of privacy. The secrecy conception of privacy may help explain the occupant’s privacy interests in images capturing her in the bedroom or bathroom, and potentially even images of her children playing in their treehouse. Her reasonable expectation of privacy exists in these places because of their inherently private nature, even if the occupant does not erect barriers to visual observations and knows a drone operates nearby. The occupant may have enough of a privacy interest in such images held by the drone software provider to prevent the application of third-party doctrine.

An analysis of the occupant’s privacy interests in drone-captured photos does not stop here. In an age of social media, someone who posts pictures of an otherwise private space is arguably sharing that space with the public. At least within the scope of that photo (and maybe beyond), the occupant’s privacy interests in that space are severely diminished. When an occupant uses a monitored home security system that videos portions of the home not visible to the public, the occupant has diminished her privacy interest in exchange for (hopefully) an increased sense of security in the home. That footage, though, is potentially subject to being shared with third parties, or even warrantless disclosure to law enforcement.

---

334. See supra section IV.C.4.
agencies. Even if an occupant has a privacy interest in drone-captured images of the home, the mere existence of images of the same spaces in another’s possession may result in the application of the third-party doctrine over the occupant’s objections.

Drone operators have the greatest ability to prevent the dissemination of drone-captured images. They must, however, take steps to prevent the drone software provider from obtaining the images in the first place. The drone operator must both not share the images with drone software provider and delete them from the operator’s own records. In Austria, recreational drone operators must default to this software configuration absent regulatory authorization. If the drone-captured images exist in some location, there is a strong likelihood that the third-party doctrine can apply to them.

One more note on the third-party doctrine. Preventing application of the third-party doctrine in criminal cases involving drone-captured images presents a paradox. If the occupant who is the subject of the voyeurism has no other means to become aware of the image capture, then the drone software provider may be in the best position to inform law enforcement of the voyeurism. By the drone software provider’s warrantless sharing of the images with law enforcement, a successful prosecution of the voyeur is much more likely. To advocate for an occupant’s privacy interests under the voyeurism statute, the drone software provider must violate
the very privacy interests that would prevent the application of the third-party doctrine.

For all these reasons, the flow of drone data interacts with the third-party doctrine to further demonstrate that privacy jurisprudence forces occupants to make difficult decisions between enjoying use of their property and enjoying protections from unwanted visual observations of the home.

V. THE PRIVACY IMPACT UNIQUE TO DRONES

Drones are distinct from manned aircraft because of their combination of minimum safe altitude of lawful operations, maneuverability, required training, operator intent, and detectability.\(^\text{340}\) With this combination of features, drones can lawfully operate in spaces that allow for image capture distinct from the capabilities of observers on the ground, manned aerial photography, satellites, and even a neighbor’s elevated vantage points.\(^\text{341}\) When considering the privacy protections enjoyed in and around the home, drones are the only technology that may be able to make visual observations of spaces in the dwelling not otherwise visible to the public without trespassing.\(^\text{342}\) Even in spaces in the dwelling and curtilage that are possibly visible to the public, drones challenge the privacy expectations of occupants in a manner distinct from any other visual observation method or technology because no temporary or incomplete physical barrier will effectively prevent unwanted visual observations.\(^\text{343}\) In the instance of children in treehouses, drones offer the possibility of image capture inaccessible to other vantage points and technologies. This, combined with the difficulties of erecting physical barriers to unwanted visual observations, means that drones may uniquely impact the privacy of children in treehouses.\(^\text{344}\) Once an image of one of these spaces has been captured, the drone operating software typically shares it with the drone software provider. The distribution of this image may trigger the third-party doctrine further challenging one’s privacy interests in and around the home.

\(^{340}\) See supra section III.A.
\(^{341}\) See supra section III.B.
\(^{342}\) See supra section IV.B.1.
\(^{343}\) See supra section III.B.
\(^{344}\) See supra section IV.B.4.
Considering the full scope of all possible visual observations of the home, the privacy impact of drones is quite limited. Depending on a specific home’s barriers to visual observation and the location of neighbor’s fixed vantage points, drones may not have a unique privacy impact at all. The occupant already enjoys no freedom from visual observation in a fence-less yard or in spaces visible from manned aircraft operating at altitudes of at least 400 feet. For those spaces visible to a neighbor, it is not clear that a drone impacts privacy any more than the neighbor’s fixed vantage points do.

Even in those spaces that are possibly visible to the public, government actors can already make warrantless observations. Occupants only have limited protections from unwanted visual observations by private actors in these spaces. If the observer has the requisite intent to violate a voyeurism statute, trigger a privacy tort, or create a private nuisance, then drones do little to challenge the protections from unwanted visual observations. Without the requisite intent, it is not clear that the lawful operation of a drone impacts an occupant’s privacy in places possibly visible to the public.

Once an image exists, the third-party doctrine turns on the question of whether it has been knowingly shared with others. Aside from aerial photography, other image capture platforms distribute images similarly to how drone operating software programs do. NASA shares updated images captured from the Landsat 8 satellite on a regular basis. Cellular phones often run backup programs that share images captured on the phone with third-party software providers.\textsuperscript{345} Under each of these circumstances the third-party doctrine may apply. Drone-captured images, therefore, are not necessarily unique in how the third-party doctrine might apply to them.

Absent an occupant’s extreme efforts to prevent public views of her home, drones impact privacy no differently than other means of image capture. The unique privacy impact of drones, therefore,

takes a peculiar shape. The current privacy jurisprudence requires that an occupant erect physical barriers in and around the home to prevent all other unwanted visual observations. As discussed, this presents a very difficult choice between enjoying her property and erecting structures that prevent all unwanted visual observations.

If an occupant goes to these lengths, then lawful drone operations can have a unique impact on privacy. Compounding this impact, drone-captured images often become the business records of drone software providers, allowing for the application of the third-party doctrine. Drones did not create these legal circumstances, but simply serve to stretch the reasoning behind the jurisprudence to its logical extreme. Legislative efforts to address the privacy impact of drones must aim either to address the unique privacy impact of drones, or to change privacy doctrines. Otherwise, the legislation does little to affect the privacy impact of drones.

VI. AN ANALYSIS OF STATE AND LOCAL STATUTES THAT SEEK TO ADDRESS DRONE PRIVACY ISSUES

As discussed, federal authorities have not enacted drone-specific laws focused on privacy in the home.346 This analysis, therefore, examines drone-specific state and local laws that impact a drone operator's ability to make visual observations of another's home. These laws fall into five distinct groupings, each limiting (1) where drones can operate, (2) under what conditions drones can capture images, (3) what images drone operators can capture, (4) drone operations by certain classes of people, and (5) the flow and uses of drone data. The Appendix contains the complete list of laws analyzed by this Article. Though there are many variations in the elements of these laws, a necessary element of each is a common actus reus—the otherwise lawful operation of a drone for the purpose of image capture.347 Before determining whether each of these categories of drone-specific laws actually has the potential to addresses the unique privacy impacts of drones, it is important to outline the assumptions upon which this analysis proceeds.

347. See supra notes 62–66 and accompanying text.
A. Assumptions

This analysis of drone-specific state and local laws is based on three hotly debated assumptions. First, the drone-specific state and local laws are not preempted by federal law and FAA regulations. Second, aside from the preemption question, each of these laws is constitutional on all other grounds, namely under the First Amendment. Third, in the application of these laws, the drone operator can be readily identified. Without these assumptions, it becomes very challenging to determine whether the drone-specific privacy laws have the potential to address the unique privacy issues presented by drones.

Regarding preemption, there are some indications that this question is settled. The FAA, in numerous public statements\textsuperscript{348} and in its notice of rulemaking for drone regulations, has taken the position that drone-specific privacy issues are the purview of states and localities.\textsuperscript{349} The FAA simply focuses its rules on the safety of drone flight operations.\textsuperscript{350} When challenged in court to promulgate drone-specific privacy regulations, the FAA has been sided with by the courts.\textsuperscript{351} It is not clear, though, that all state and local drone-specific privacy laws could completely avoid preemption by the FAA.\textsuperscript{352}

Certain state and local laws which aim to protect privacy, such as certain trespassing statutes, may encroach on the FAA’s drone flight operations remit.\textsuperscript{353} The FAA has the authority to regulate the safety of flight operations from the ground up.\textsuperscript{354} Aerial trespass, though, occurs when someone encroaches on immediate


\textsuperscript{349} Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. at 42,192.

\textsuperscript{350} Fed. Aviation Admin., supra note 348, at 1.


reaches of the atmosphere adjoining the land such as to interfere with the occupant’s enjoyment of the land. When only manned aircraft ruled the skies, a combination of legal precedents strongly suggested that an aircraft operating in public airspace did not commit aerial trespass. This broad rule has been tempered by the acquisition of avigation easements from property owners in the take-off and landing paths around airports and other aerodromes. With the introduction of drones, the question of where airspace subject to aerial trespass ends and the public airways begin has become much more complex. See Troy Rule’s article, Airspace in an Age of Drones, for an excellent analysis of this question. To avoid resolving the question of FAA preemption regarding aerial trespass, this analysis assumes that aerial trespass starts across the terrestrial property line at any altitude, unless the specific law says otherwise.

On the constitutionality front, the question of whether drone-specific privacy laws violate the First Amendment remains open. Several jurisdictions have enacted drone-specific privacy laws that may effectively ban image capture by drones under certain circumstances. Courts have recognized the right to record images as a necessary precursor to speech. Accordingly, restrictions on recordings made by drones may impinge speech rights protected by the First Amendment. Regarding freedom from visual observation in the home, these statutes may be considered overbroad. Drone image capture prohibitions directed at places other than the home—commercial facilities, public gatherings, etc.—are already

355. RESTATEMENT (SECOND) OF TORTS § 158 (AM. LAW INST. 1965); see also Rule, supra note 239, at 156.
356. United States v. Causby, 328 U.S. 256, 264 (1946); Hinman v. Pac. Air Transp., 84 F.2d 755, 758 (9th Cir. 1936); Reaver v. Martin Theaters, 52 So. 2d 682 (Fla. 1951).
357. See supra note 295.
359. See generally Rule, supra note 239.
360. See, e.g., TEX. GOV’T CODE ANN. § 423.002.
361. See Blitz et al., supra note 24, at 87–91; Kaminski, supra note 3, at 61 n.24.
362. Kaminski, supra note 3, at 61–64; Matiteyahu, supra note 4, at 283.
being challenged on First Amendment grounds. But, for the purposes of this analysis, it is assumed that none of these state and local drone-specific laws aimed at protecting the privacy of the home are unconstitutional.

The last assumption necessary for this analysis is that the occupant of the home can readily identify the drone operator. As discussed above, this is a most challenging assumption related to drones. When all parties conduct themselves lawfully, it is very difficult to identify who is operating a drone. Adding to these challenges that someone operating a drone with a privacy-invading intent may take precautions against being identified, it may be effectively impossible to identify a drone operator. Without this assumption, adjudication of any of the drone-specific privacy protections becomes incredibly challenging. The question of the efficacy of these laws in protecting against drone-specific privacy invasions would, therefore, necessarily have to address identifying the drone operator. Assuming that the drone operator can be identified, though, this analysis can focus on whether it is even possible for the drone-specific law to protect against the unique privacy impacts of drones.

B. Analysis of State and Local Laws

1. Laws That Limit Where Drones Can Operate

States and localities have adopted a variety of provisions that limit where drones can operate. At one extreme, Augusta, Georgia has banned nearly all drone operations without written permission from the Augusta city commission. The New Jersey boroughs of Allendale and Beachwood have bans on drone operations “below

---

364. But see BENNET, supra note 42, at 5.
365. See supra notes 162–73 and accompanying text.
367. See supra section IV.B.5.
368. AUGUSTA, GA., MUN. CODE § 1-3-44 (allowing one exception—drone operations over previously designated model aircraft airfields).
400 feet over residential . . . zone[s].

These laws address the unique privacy issues presented by drones by effectively preventing drones from operating in areas where they could capture images of homes. If drones cannot operate, they cannot capture images that impact privacy in and about the home.

Many municipalities have enacted laws that designate any unwanted encroachment by drone at any altitude across a terrestrial property line as trespass. Laws such as these may not prevent unwanted visual observations by drone. A drone need not cross terrestrial property lines to capture images of another’s home. The specific arrangement of visual barriers at a particular home, therefore, will determine whether laws such as these actually protect against the unique privacy impact of drones. Some states and municipalities have determined that trespass by drone takes place only when the drone both encroaches across the terrestrial property line and operates below a certain altitude. West Goshen, Pennsylvania, for example, has designated that altitude at 200 feet. In Tennessee and Wyoming, the statutes do not designate a specific altitude, but set conditions under which low flying drones would be committing trespass. Like with provisions that designate trespass at any altitude, the efficacy of these laws in addressing the unique privacy impact of drones depends entirely on the visual barriers an occupant has erected around her home.

In other words, the efficacy of these laws hinges on the presence of visual barriers necessitated by current privacy jurisprudence. Drones did not create these circumstances. Rather, current U.S.


370. E.g., Chi., Ill., Mun. Code § 10-36-400(b)(12); Telluride, Colo., Mun. Code § 10-11-30(g); Laurel Hollow, N.Y., Code § 85-9(C).

371. Franklin Lakes, N.J., Code § 137-3(A) (“Small unmanned aircraft shall not operate in any airspace below 400 feet within the Borough: (1) Over private property, without the permission of the private property owner . . . .”).

372. In Olmstead, Justice Brandeis noted in his dissent it was “immaterial where the physical connection with the telephone wires . . . was made.” Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting). By analogy to drones, it does not matter if the drone is trespassing when it makes unwanted visual observations of someone’s home. See also United States v. Jones, 565 U.S. 400, 421–22 (2012) (Alito, J. concurring).

373. See supra section IV.B.


privacy protections present those seeking relief from unwanted visual observations by drones with a nearly impossible choice.

At the other extreme of laws dictating where drones can operate, Nevada, Oregon, Utah, and Virginia have made trespass by drone illegal only after the occupant has provided the drone operator notice that such encroachment is unwanted. These laws do little to prevent unwanted visual observations by drones for two reasons. First, as with laws that define trespass at the terrestrial property lines, the efficacy of such laws depends on the particular physical barriers that an occupant has erected around her home. Second, even if the occupant sees the drone on its first flight over the occupant’s home, that flight is not unlawful under these statutes. The drone operator can keep making unwanted visual observations of the occupant’s home until the occupant specifically tells the drone operator to stop. When considering the property theory and surveillance conception of privacy, even the possibility of a single lawful image capture means that these laws effectively offer no protection from unwanted visual observations. These laws only offer some protection from unwanted visual observations under the reasonable expectations theory and secrecy conception of privacy because the occupant expresses her desired level of privacy by asking the drone operator to stop.

2. Laws That Limit Under What Conditions Drones Can Capture Images

Another group of laws prohibits using a drone to capture images without the consent of the subject of the image capture. States like Idaho, Tennessee, and Texas require permission to capture images of an occupant’s home. Chicopee, Massachusetts requires consent for drone image capture of any person, regardless of whether

377. See supra notes 372–374 and accompanying text.
378. When considering the difficulty in both detecting a drone and identifying a drone operator, these statutes’ ability to protect privacy becomes even more limited. See supra section III.A.5.
379. See supra sections IV.C.1, IV.C.2.
they are in their home.\footnote{Chicopee, Mass., Code § 186-4(C)(7).} These laws acknowledge that drones are primarily data collection devices and that operators have to demonstrate very little intent in order to make visual observations of others.\footnote{See supra section III.A.4.} By creating a presumption that image capture is not permitted, these laws require the drone operator to first notify occupants of the intended image capture. The burden of preventing unwanted visual observation falls on the drone operator, not the occupant of the home having to erect barriers that deprive her of enjoyment of her property. At that point an occupant knows that drone image capture may take place and can decide whether to grant permission to the drone operator. If these laws work as intended, they have the potential to be very effective in preventing unwanted visual observations via drone of occupants in and about their homes.

3. Laws That Limit What Images Drone Operators Can Capture

The next group of laws limits what images drone operators can capture. For the purposes of this discussion, it is assumed that the occupant has not provided her consent for the image capture.\footnote{For this group of laws, the occupant’s lack of consent, either explicit or implied by virtue of the subject matter of the image, tends to be a necessary element for a successful cause of action. E.g., Fla. Stat. Ann. § 934.50(3)(b); 18 Pa. Cons. Stat. § 3505(a)(1).} Some of these laws focus on the content of the images. Wisconsin and Hermosa Beach, California ban the use of drones to capture any image of a space where the occupant has a “reasonable expectation of privacy.”\footnote{E.g., Wis. Stat. § 942.10; Hermosa Beach, Cal., Mun. Code § 9.38.040(H).} It is not clear that such provisions actually prevent unwanted visual observations from drones. The question of the occupant’s reasonable expectation of privacy depends on both the visual barriers she has erected around her home and which line of reasoning the court will apply to determine reasonable expectations of privacy.\footnote{See supra sections IV.C, IV.D.} If a court uses the line of reasoning found in \textit{Ciraolo} and \textit{Riley}, the failure to erect a complete visual barrier means that the occupant has no reasonable expectation of privacy.\footnote{See supra notes 323–25 and accompanying text.} Provisions like these, therefore, arguably do little to address the unique privacy impact of drones.
The West Virginia statute, for example, addresses this issue by specifying that an invasion of privacy happens when a drone operator captures or records an image “through a window.” Burbank, California takes a similar approach because images cannot be captured of “an enclosed area from public view such as fenced backyards or the interior of any structure.” Provisions like these help address the unique privacy issues presented by drones because they attempt to prevent image capture of spaces accessible to visual observation by drones, even if the occupant has not erected complete visual barriers.

The largest number of drone-specific laws that affect unwanted visual observations of the home focus on the drone operator’s intent. The content of drone-captured images violate these laws because the drone operator captured them with the intent to commit surveillance, stalking, harassment, voyeurism, or invasion of privacy. By focusing on the drone operator’s intent these laws place less emphasis on the visual barriers erected by occupants around their homes. Drone operators with improper intents cannot take advantage of drones’ unique abilities to capture images from vantage points inaccessible by other means or technologies. Like their non-drone-specific counterparts, it is difficult to enforce these laws because the act of merely operating the drone and (nearly automatically) capturing images with it may not be enough to establish the drone operator’s illegal intent. In short, if intent can be established by other means then these laws take an important step to address the unique privacy issues presented by drones.

388. W. VA. CODE § 61-16-2(1).
389. BURBANK, CAL., CODE § 5-3-1602(M) (using these examples, presumably “public view” means ground-level observations only).
390. E.g., N.D. CENT. CODE § 29-29.4-05(2)(a); CUYAHOGA HEIGHTS, OHIO, CODE § 650(02)(b).
391. E.g., N.J. STAT. ANN. § 2C:40-28(g); HERMOSA BEACH, CAL., MUN. CODE § 9.38.040(M).
392. E.g., DEL. CODE ANN. tit. 11, § 1334(b)(4); Defuniak Springs, Fla., Ordinance 866 § 3.E.3 (May 23, 2016).
393. E.g., ARK. CODE ANN. § 5-16-102(b); MISS. CODE ANN. § 97-29-61(1)(b).
394. E.g., CAL. CIV. CODE § 1708.8; Ada County, Idaho, Ordinance 883 § 3 (May 15, 2018).
395. See supra note 17 and accompanying text; Miller, supra note 1, at 353.
396. See Scharf, supra note 23, at 1101; Friedenzohn & Branum, supra note 3, at 401 (“It would be difficult for a party to argue that the use and enjoyment of their property is affected by a UAS flying somewhere near their property.”); see also supra section III.A.4.
4. Laws That Limit Drone Operations by Certain Classes of People

A smaller group of laws specifically restricts image capture by drone based on the classification of the drone operator. In several states, individuals who are subject to judicial protective orders, like restraining orders, may not use drones to capture images in violation of such orders. For the individuals these judicial orders seek to protect, these statutes help address the unique privacy issues presented by drones. By specifically listing drone use as a means of violating these orders, the individuals protected by these orders do not have to block all possible visual observations by drones in order to protect their own privacy interests against invasions by specific individuals.

If an individual is a registered sex offender in Indiana, Michigan, or Virginia, that person’s ability to use a drone may be significantly proscribed. If such an individual seeks to capture images of occupants in a home it may violate one of these statutes. The occupant’s efforts to block visual observations do not factor into these laws. Accordingly, such laws can help address the unique privacy issues presented by drones.

In Texas a real estate broker or land surveyor can only capture images via drone if it is within the scope of her professional practice and no individuals can be identified in the images. Capturing images of homes is an important activity in both these professions. Even though an occupant’s property appears in the field of view of a drone-captured image, at least no images of the occupant herself can be used by the real estate broker or surveyor. These provisions, therefore, have some effect on the unique privacy issues presented by drones.

397. *E.g.*, DEL. CODE ANN. tit. 11, § 1334(b)(6); IND. CODE § 35-46-1-15.1(a)–(b); MICH. COMP. LAWS § 259.322(2); N.J. STAT. ANN. § 2C:40-28(f).

398. It is worth noting, though, that the detectability issues presented by drones may make enforcement of these statutes more challenging. *See supra* section III.A.5.

399. IND. CODE § 35-42-4-12.5(b); MICH. COMP. LAWS § 259.322(4); VA. CODE ANN. § 18.2-324.2(A).

400. TEX. GOV’T CODE ANN. § 423.002(13)(19).
5. Laws That Limit the Flow and Uses of Drone Data

Some jurisdictions, recognizing the inherent data-collection qualities of drones, have enacted legislation specifically aimed at limiting how data might flow from a drone. In Idaho and Laurel Hollow, New York, for example, a drone operator cannot publish or otherwise publicly disseminate a drone-captured image of an individual without her consent.\textsuperscript{401} It is important to examine these provisions in light of the fact that drone software providers often have automatic access to drone-captured images.\textsuperscript{402} This feature of drones means that the drone-captured image may instantly be transmitted from the operator’s drone or phone to computer facilities under the drone software provider’s control.\textsuperscript{403} The drone software provider may share the images on a public forum\textsuperscript{404} or sell the images.\textsuperscript{405}

Accordingly, the act of capturing an image via drone is tantamount to disclosing, displaying, distributing, or otherwise using that image.\textsuperscript{406} If a jurisdiction has this understanding of drone data flows, then this law effectively prevents image capture without the occupant’s permission.\textsuperscript{407} Occupants do not have to erect visual barriers around their homes to enjoy a privacy interest in a drone-captured image. Rather, the drone operator simply has a duty not to share the images. Hence, the third-party doctrine has limited effects. In that way, this provision helps address the unique privacy issues presented by drones.

Even if a jurisdiction views drone image capture and drone image publishing as separate acts, the requirement to obtain the occupant’s permission to distribute the images has some effect on the unique privacy issues presented by drones. Because of the permission requirement, the occupant has some agency in how images of

\textsuperscript{401} Idaho Code § 21-213(2)(b); Laurel Hollow, N.Y., Code § 85-9(B).

\textsuperscript{402} See supra note 141 and accompanying text.

\textsuperscript{403} See Barstow, Cal., Code § 9.66.020(d) (banning transmission of drone-captured images); Manhattan Beach, Cal., Code § 3.70.030(A) (banning transmission of drone-captured images).

\textsuperscript{404} DJI Privacy Policy, supra note 17 (discussing the SkyPixel image sharing forum).

\textsuperscript{405} See supra note 322.


\textsuperscript{407} See Scharf, supra note 23, at 1102–03.
herself or her home are distributed, particularly under a reasonable expectations theory or secrecy conception of privacy. This effectively provides some privacy protection independent of what visual barriers she may have erected around her home.

Focusing more directly on the third-party doctrine, some states have passed laws that limit law enforcement’s ability to use drone-captured images. These laws often prevent law enforcement from obtaining drone-captured images, even from private drone operators, except pursuant to a warrant. Some states allow for the full range of exceptions to the warrant requirement, while others offer just a few exceptions and others directly limit the admissibility of drone-captured images from private operators.

These statutes have some effect on the unique privacy issues created by drones. Even if a drone-captured image of the occupant’s home exists, each of these provisions presents a barrier to government access to the photo without a warrant. Rather than simply being able to subpoena drone-captured images held by third parties, the government actor must consider whether a warrant is required. That analysis leads to a review of any applicable warrant exceptions. If the content of the images includes parts of the home considered in “plain view,” then a warrant requirement is ineffectual because current privacy jurisprudence dictates any part of the home is in “plain view” unless it is behind a complete visual barrier. Accordingly, the existence of the photo may be enough grounds for finding a warrant exception, thereby leaving the unique privacy issues presented by drones effectively unaddressed. Only statutes that limit government access or use of drone-captured images and limit the warrant exceptions can have an effect on unique privacy issues presented by drones.

408. See supra sections IV.C.3, IV.C.4.
409. Kaminski, supra note 3, at 66; infra note 410.
410. E.g., Fla. Stat. § 934.50(4)(b); Wis. Stat. § 175.55(2).
411. E.g., Iowa Code § 808.15; Mont. Code Ann. § 46-5-109(1); N.D. Cent. Code § 29-29.4-02.
414. See supra note 259 and accompanying text.
C. Third-Party Doctrine Revisited

Laws on government use of drone-captured images are not the only statutes that may affect the application of the third-party doctrine. All the state and local laws discussed in this Part VI help define an occupant’s privacy interests in the drone-captured images. Taking all the drone-specific state and local laws into account, the occupant has the strongest privacy interest in images of the home when the following eight factors are present:

1. the drone operator has limited authorization, based on her status (profession or judicial orders), to capture images of the home in question;\(^{415}\)

2. the occupant has blocked public observation of the space in question from visual observations made from the ground, the air, and the neighbors’ fixed vantage points;\(^{416}\)

3. the occupant has not granted the drone operator permission to capture the images;\(^{417}\)

4. the occupant lives in a jurisdiction that requires specific authorization to share data gathered by drones;\(^{418}\)

5. the drone operator captures the images with a privacy-invading intent;\(^{419}\)

6. the occupant has not previously shared (either herself or through prior authorization to another) images of the space in question;\(^{420}\)

7. the jurisdiction in question has a warrant requirement for use of drone-obtained data (including images);\(^{421}\) and

8. no warrant exceptions apply to the facts and circumstances in question.\(^{422}\)

\(^{415}\) See supra section VI.B.4.
\(^{416}\) See supra Part V.
\(^{417}\) See supra section VI.B.2.
\(^{418}\) See supra section VI.B.5.
\(^{419}\) See supra section VI.B.3.
\(^{420}\) See supra section IV.D.
\(^{421}\) See supra section VI.B.5.
\(^{422}\) See supra section VI.B.5.
This list proceeds roughly along the timeline of drone data flows to identify the points where laws and other legal doctrines may be asserted to protect the occupant’s privacy interests. Starting with rules affecting the drone operator, if the drone operator is not permitted to capture images of the home in question, then the occupant’s privacy interests can be protected independent of any steps the occupant may have taken or failed to take. If the operator is permitted to fly the drone, the next question revolves around the physical layout of the occupant’s home. Consistent with current jurisprudence, the occupant would have a difficult time asserting a privacy interest in observations made from a public vantage point. Even if the drone operator had a privacy invading intent, it would be difficult to find evidence of that intent from such images because the occupant did not erect adequate barriers to prevent visual observations from public vantage points. If the occupant clears this (rather high) hurdle, in some jurisdictions the privacy protection burden moves back to the drone operator because the occupant has to authorize the capture of images of her home. The privacy-invading nature of the drone observation, though, may be impacted by whether the occupant shared images of her home at another time. Accordingly, it may be difficult for an occupant to assert a privacy interest in images that she has already shared. If the occupant still has a privacy interest in drone-captured images after all these circumstances have been considered, then government actors may need a warrant to obtain the drone-captured images in question. At this point, warrant exceptions or restrictions on images captured from drones come into play relative to the occupant’s privacy interest.

In short, aside from the first factor, if any of the other factors are absent, then the occupant’s privacy interest in the images captured by a drone is diminished and the third-party doctrine may be applied. With each diminishment in privacy interests, law enforcement’s warrant requirement to access the images captured by the drone also diminishes. Figure 3 presents a decision tree that outlines the three possible outcomes relative to drone-captured images and the third-party doctrine.
### Figure 3—Drone-Captured Images and the Third-Party Doctrine

#### Decision Tree

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1: Is the person operating the drone someone with limited legal right to capture images of the home or occupant in question?</td>
<td>Proceed to #2</td>
<td>Proceed to #3</td>
</tr>
<tr>
<td>#2: Does the local law allow the person with limited legal rights to obtain permission to use the drone to capture images of the home or occupant in question?</td>
<td>Proceed to #4</td>
<td>Proceed to #8—occupant’s privacy interest is strong</td>
</tr>
<tr>
<td>#3: Has the occupant asserted a privacy interest in those portions of the home subject to image capture by blocking them from all public ground-level observations, all aerial observations, and each of the neighbors’ fixed vantage points?</td>
<td>Proceed to #4</td>
<td>Proceed to #9—occupant’s privacy interest is diminished</td>
</tr>
<tr>
<td>#4: Was the image captured with the occupant’s permission?</td>
<td>Proceed to #5</td>
<td>If arriving from #3, proceed to #6; if arriving from #2, proceed to #8—occupant’s privacy interest is strong</td>
</tr>
<tr>
<td>#5: Did the permission include the authorization to share the images or other drone data?</td>
<td>Proceed to #9—occupant’s privacy interest is diminished</td>
<td>Proceed to #7</td>
</tr>
<tr>
<td>#6: Was the image captured with a privacy-invading interest?</td>
<td>Proceed to #8—occupant’s privacy interest is strong</td>
<td>Proceed to #7</td>
</tr>
<tr>
<td>#7: Does the law in that jurisdiction require occupant authorization to share drone data?</td>
<td>Proceed to #8—occupant’s privacy interest is strong</td>
<td>Proceed to #9—occupant’s privacy interest is diminished</td>
</tr>
<tr>
<td>#8: Has the occupant previously shared (published or authorized another to capture) images of the private space in question?</td>
<td>Proceed to #9—occupant’s privacy interest is strong</td>
<td>Option A</td>
</tr>
<tr>
<td>#9: Does the jurisdiction have any warrant requirements for law enforcement use of drone data?</td>
<td>Proceed to #10</td>
<td>Option B</td>
</tr>
<tr>
<td>#10: Do any warrant exceptions, based on the law or the facts and circumstances, apply to this image?</td>
<td>Option B</td>
<td>Option C</td>
</tr>
</tbody>
</table>

#### Option A: Third-Party Doctrine Unlikely to Apply
The occupant has a strong privacy interest in the images. Therefore, barring other circumstances, law enforcement likely needs a warrant to obtain the images.

#### Option B: Third-Party Doctrine Likely to Apply
The occupant has a diminished privacy interest in the images. Therefore, it is unlikely that law enforcement would need a warrant to obtain the images.

#### Option C: Third-Party Doctrine Could Possibly Apply
The occupant has a diminished privacy interest in the images, but some other factor may require that law enforcement obtain a warrant to obtain the images. Therefore, the particular circumstances will dictate whether the third-party doctrine applies.
As one can see from Figure 3, there are few circumstances under which an occupant will have a strong privacy interest in drone-captured images. The biggest obstacle for avoiding application of the third-party doctrine arises at Question 3—erecting all the necessary visual barriers to prevent unwanted visual observations. As discussed throughout this Article, drones did not create this requirement. Rather the existing privacy jurisprudence effectively forces people seeking freedom from unwanted visual observations to keep their blinds closed and make their curtilage an indoor space. If someone does not meet this requirement, only limitations to warrant exceptions could prevent the full application of third-party doctrine.

If someone has erected all the necessary physical barriers, then state and local legislative efforts help preserve those privacy interests. The analysis reveals that there are still many opportunities to diminish one’s privacy interests. In other words, unless all the correct conditions align there is at least a chance that the third-party doctrine could be applied. In principle, the combination of all these laws has some impact on the unique privacy issues presented by the lifecycle of drone-captured data. To the best of the author’s knowledge no single state has all these laws in place. The application of all these privacy protections as presented here, therefore, is merely theoretical. Until a state enacts the full complement of these laws, occupants will effectively have no privacy interests in drone-captured data that can survive application of the third-party doctrine.

CONCLUSION

This Article sought to demonstrate that the privacy impact of drones is really very limited. Starting with a precise definition of drones, drones were distinguished from manned aircraft, other image capture technologies, and even a neighbor’s elevated vantage points. When moving through the spaces of the home that enjoy different levels of privacy protection, the unique privacy impact of drones becomes clear—drones impact privacy uniquely when they make visual observations not accessible to other technologies and

423. There may be some local jurisdictions that have all these provisions in place, particularly in Tennessee or California. The author has not conducted the exhaustive research required to find these specific localities.
methods. Relatively few factual circumstances create this possibility. Accordingly, drones have a limited impact on privacy.

The current U.S. privacy jurisprudence requires that an occupant make both her dwelling and her curtilage impervious to visual observations. Drones did not create these conditions. Rather, drones highlight the logical conclusion that one must draw from the application of existing privacy doctrines.

Drones are primarily information gathering devices, so the flow of data from drones was important to this Article. Absent complete barriers to visual observation and the happenstance of living in a jurisdiction with strong drone-specific privacy protections, the third-party doctrine likely applies to most drone-captured images. Accordingly, people who are the subject of drone-captured images have almost no recourse to prevent the sharing of those images with the government or other parties.

Considering these legal and factual realities, efforts to address the privacy issues raised by drones can proceed on two fronts. Legislation can limit drones’ ability to capture data. Other countries have taken this approach. In the U.S. though, First Amendment concerns would likely limit the applicability of such laws to drone image capture of the visible light spectrum. Legislation that limits drones’ ability to capture other parts of the electromagnetic spectrum (e.g., infrared, ultraviolet, radio frequencies), audio frequencies, or chemical sensing would likely have fewer First Amendment issues.

If legislation cannot effectively limit drones’ ability to capture images of the visual light spectrum, then the only other way to address the privacy impact of drones is to change privacy doctrine. Drones highlight the fact that privacy jurisprudence requires the occupant of a home to erect complete physical barriers to prevent unwanted visual observations. The third-party doctrine only exacerbates the effects of this requirement. Both the privacy jurisprudence and the third-party doctrine arose from cases that did not involve drones, but those cases discussed the very issues highlighted by drones. Accordingly, it is not fair to say that drones are impacting privacy in a unique way when the cases that form the basis of U.S. privacy protections contemplated the present circumstances. A combination of changes to the privacy doctrine and the third-party doctrine could strike a better balance between lawful drone operations and the privacy protections afforded to people in the United States.
APPENDIX

DRONE-SPECIFIC STATE AND LOCAL LAWS IMPACTING PRIVACY OF THE HOME

<table>
<thead>
<tr>
<th>Laws That Limit Where Drones Can Operate</th>
</tr>
</thead>
<tbody>
<tr>
<td>PARADISE VALLEY, ARIZ., TOWN CODE §§ 10-12-1 et seq.</td>
</tr>
<tr>
<td>BARSTOW, CAL., Code § 9.60</td>
</tr>
<tr>
<td>BURBANK, CAL., Code § 5-3-16-02</td>
</tr>
<tr>
<td>HERMOSA BEACH, CAL., MUN. CODE §§ 9.38.010 et seq.</td>
</tr>
<tr>
<td>LOS ALAMITOS, CAL., MUN. CODE §§ 8.52.010 et seq.</td>
</tr>
<tr>
<td>WEST HOLLYWOOD, CAL., Code § 9.30.040</td>
</tr>
<tr>
<td>CHERRY HILLS VILLAGE, COLO., CODE § 5-3-16-02</td>
</tr>
<tr>
<td>TELLURIDE, COLO., MUN. CODE §§ 10.11.10 et seq.</td>
</tr>
<tr>
<td>DEL. CODE ANN. tit. 11, § 1334</td>
</tr>
<tr>
<td>Defuniak Springs, Fla., Ordinance 866 (May 23, 2016)</td>
</tr>
<tr>
<td>AUGUSTA, GA., MUN. CODE §§ 1-3-44 et seq.</td>
</tr>
<tr>
<td>WARNER ROBINS, GA., CODE §§ 13-102, -103</td>
</tr>
<tr>
<td>CHI., ILL., MUN. CODE § 10-36-400</td>
</tr>
<tr>
<td>ROLLING MEADOWS, ILL., CODE § 38-355</td>
</tr>
<tr>
<td>PRAIRIE VILLAGE, KAN., CODE §§ 11-1601 et seq.</td>
</tr>
<tr>
<td>CHICOPEE, MASS., CODE § 186-4</td>
</tr>
<tr>
<td>HOLYOKE, MASS., CODE OF ORDINANCES § 54-22</td>
</tr>
<tr>
<td>MICH. COMP. LAWS ANN. § 259.320</td>
</tr>
<tr>
<td>CITY OF EAST LANSING, MICH., CODE § 26-67</td>
</tr>
<tr>
<td>SAINT BONIFACIUS, MINN., CODE OF ORDINANCES §§ 91-01 et seq.</td>
</tr>
<tr>
<td>CITY OF WILDWOOD, MO., CODE § 236.010</td>
</tr>
<tr>
<td>NEV. REV. STAT. §§ 493.103, .109</td>
</tr>
<tr>
<td>ALLENDALE, N.J., MUN. CODE §§ 118-2, .3</td>
</tr>
<tr>
<td>Beachwood, N.J., Ordinance 2016-04 (Mar. 16, 2016)</td>
</tr>
<tr>
<td>FRANKLIN LAKES, N.J., CODE §§ 137-1 et seq.</td>
</tr>
</tbody>
</table>
### Laws That Limit Under What Conditions Drones Can Capture Images

<table>
<thead>
<tr>
<th>State</th>
<th>Ordinance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arkansas</td>
<td>§ 5-16-101(b)</td>
</tr>
<tr>
<td>Defuniak Springs, Fla.</td>
<td>Ordinance 866 (May 23, 2016)</td>
</tr>
<tr>
<td>Idaho</td>
<td>§ 21-213</td>
</tr>
<tr>
<td>Louisiana</td>
<td>§ 14:63</td>
</tr>
<tr>
<td>City of Chicopee, Mass.</td>
<td>§ 186-4</td>
</tr>
<tr>
<td>Holyoke, Mass.</td>
<td>Code of Ordinances § 54-22</td>
</tr>
<tr>
<td>Alldendale, N.J.</td>
<td>Mun. Code §§ 118-2, -3</td>
</tr>
<tr>
<td>Beachwood, N.J.</td>
<td>Ordinance 2016-04 (Mar. 16, 2016)</td>
</tr>
</tbody>
</table>
Laws That Limit What Images Drone Operators Can Capture

ARK. CODE ANN. §§ 5-16-101(b), -102(b)
CAL. CIV. CODE § 1708.8
BARSTOW, CAL., CODE § 9.66
BURBANK, CAL., CODE § 5-3-16-02
HERMOSA BEACH, CAL., MUN. CODE §§ 9.38.010 et seq.
MANHATTAN BEACH, CAL., CODE § 3.7.030
WEST HOLLYWOOD, CAL., CODE § 9.30.040
TELLURIDE, COLO., MUN. CODE §§ 10-11-10 et seq.
DEL. CODE ANN. tit. 11, § 1334
BETHANY BEACH, DEL., CODE § 212-6(10)
FLA. STAT. § 934.50
AVENTURA, FLA., CODE OF ORDINANCES § 30.211
Defuniak Springs, Fla., Ordinance 866 (May 23, 2016)
<table>
<thead>
<tr>
<th>Code</th>
<th>Ordinance/Section</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDAHO CODE 21-213</td>
<td>Ada County, Idaho, Ordinance 883 (May 15, 2018)</td>
<td></td>
</tr>
<tr>
<td>CHI., ILL., MUN. CODE 10-36-400</td>
<td>Rolling Meadows, ILL., Code 38-355</td>
<td></td>
</tr>
<tr>
<td>IND. CODE §§ 35-45-4-5, -10-6</td>
<td>KAN. STAT. ANN. § 60-31A02</td>
<td></td>
</tr>
<tr>
<td>PRAIRIE VILLAGE, KAN., CODE §§ 11-1601 et seq.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LA. STAT. ANN. § 14:63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LA. STAT. ANN. § 14:283</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LA. STAT. ANN. §§ 14:283.1, -3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LA. STAT. ANN. § 14:284</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEST MONROE, LA., CODE § 11-5017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MICH. COMP. LAWS § 259.322</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAST LANSING, MICH., CODE § 26-67</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLUSHING, MICH., CODE § 132.02(8)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MISS. CODE ANN. § 97-29-61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LONG BEACH, N.J., CODE §§ 57-2, -3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HUNTINGTON, N.Y., CODE § 189</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAUREL HOLLOW, N.Y., CODE § 85-9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NORTHPORT, N.Y., CODE § 313</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N.C. GEN. STAT. § 15A-300.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N.D. CENT. CODE § 29-29.4-05</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOTTINEAU, N.D., CODR § 10.0902</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUYAHOGA HEIGHTS, OHIO, CODE § 650</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NICHOLS HILLS, OKLA., CODE § 32-188</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR. REV. STAT. § 837.370</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR. REV. STAT. § 163.700</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 PA. CONS. STAT. § 3505</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.D. CODIFIED LAWS § 22-21-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABERDEEN, S.D., CODE OF ORDINANCES § 10-2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Laws That Limit Drone Operations by Certain Classes of People

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENN. CODE ANN. § 39-13-903</td>
<td></td>
</tr>
<tr>
<td>TEX. GOV’T CODE ANN. § 423.003</td>
<td></td>
</tr>
<tr>
<td>UTAH CODE ANN. § 76-9-402</td>
<td></td>
</tr>
<tr>
<td>W. VA. CODE § 61-16-2</td>
<td></td>
</tr>
<tr>
<td>WIS. STAT. § 942.10</td>
<td></td>
</tr>
<tr>
<td>ELKHART LAKE, WIS., CODE § 26.05</td>
<td></td>
</tr>
<tr>
<td>GREENFIELD, WIS., CODE OF ORDINANCES § 10.35</td>
<td></td>
</tr>
<tr>
<td>HUDSON, WIS., MUN. CODE § 187-20</td>
<td></td>
</tr>
<tr>
<td>WYO. STAT. ANN. § 10-4-303</td>
<td></td>
</tr>
</tbody>
</table>

Laws That Limit the Flow and Uses of Drone Data

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PARADISE VALLEY, ARIZ., TOWN CODE §§ 10-12-1 et seq.</td>
<td></td>
</tr>
<tr>
<td>BARSTOW, CAL., CODE § 9.60</td>
<td></td>
</tr>
<tr>
<td>HERMOSA BEACH, CAL., MUN. CODE §§ 9.38.010 et seq.</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Code or Statute Details</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Manhattan Beach, Cal.</td>
<td>Code § 3.7.030</td>
</tr>
<tr>
<td>Fla. Stat. § 934.50</td>
<td></td>
</tr>
<tr>
<td>Defuniak Springs, Fla.,</td>
<td>Ordinance 866 (May 23, 2016)</td>
</tr>
<tr>
<td>IOWA CODE § 808.15</td>
<td></td>
</tr>
<tr>
<td>Idaho Code § 21-213</td>
<td></td>
</tr>
<tr>
<td>Ada County, Idaho, Ordinance 883</td>
<td>(May 15, 2018)</td>
</tr>
<tr>
<td>725 ILL. COMP. STAT. 167/40</td>
<td></td>
</tr>
<tr>
<td>IND. CODE § 35-33-5-10</td>
<td></td>
</tr>
<tr>
<td>IND. CODE § 35-45-5-5</td>
<td></td>
</tr>
<tr>
<td>LA. STAT. ANN. § 14:283</td>
<td></td>
</tr>
<tr>
<td>LA. STAT. ANN. § 14:283.3</td>
<td></td>
</tr>
<tr>
<td>Saint Bonifacius, Minn.,</td>
<td>Code of Ordinances §§ 91-01 et seq.</td>
</tr>
<tr>
<td>Mont. Code Ann. § 46-5-109</td>
<td></td>
</tr>
<tr>
<td>Nev. Rev. Stat. § 493.112</td>
<td></td>
</tr>
<tr>
<td>Huntington, N.Y., Code § 189</td>
<td></td>
</tr>
<tr>
<td>Laurel Hollow, N.Y., Code § 85-9</td>
<td></td>
</tr>
<tr>
<td>Northport, N.Y., Code § 313</td>
<td></td>
</tr>
<tr>
<td>N.C. Gen. Stat. § 15A-300.1</td>
<td></td>
</tr>
<tr>
<td>N.D. Cent. Code Ann. § 29-29-4-02</td>
<td></td>
</tr>
<tr>
<td>Cuyahoga Heights, Ohio, Code § 650</td>
<td></td>
</tr>
<tr>
<td>Or. Rev. Stat. § 837.320</td>
<td></td>
</tr>
<tr>
<td>Tex. Gov’t Code Ann. §§ 423.004,</td>
<td></td>
</tr>
<tr>
<td>Utah Code Ann. § 72-14-203</td>
<td></td>
</tr>
<tr>
<td>VT. Stat. Ann. tit. 20 § 4622</td>
<td></td>
</tr>
</tbody>
</table>