REMOTE SENSING OF PRIVATE DATA BY DRONES IS MOSTLY UNREGULATED: REASONABLE EXPECTATIONS OF PRIVACY ARE AT RISK ABSENT COMPREHENSIVE FEDERAL LEGISLATION

JOSEPH J. VACEK, J.D., CFI*

ABSTRACT

The current regulatory structure governing the use of small drones by government and citizens is not yet fully settled, but enough parameters exist in the form of existing and proposed regulations, statutes, and case law that the answer to the question of whether police and private citizens may use small drones to remotely sense or record other people's activities is generally yes, subject to a few limitations. The next set of questions that arise pertain to the methods of collection, use, retention, and dissemination of that remotely sensed data. The current legal landscape in the United States relevant to that set of questions includes common law principles based in tort, the Third-Party Doctrine, federal data protection statutes such as the Electronic Communications Privacy Act and the Privacy Act, Unmanned Aircraft System-specific laws, policies and regulations such as the 2012 FAA Reauthorization Act, the newly proposed Federal Aviation Regulations for small UAS, and a Presidential Memorandum on privacy issues related to drone use. Those laws, regulations, and policies, both individually and together, are ineffective in protecting remotely sensed private data. Because states are federally preempted from regulating aviation, a comprehensive federal legislative enactment delineating specific limitations on the gathering of private data via drones is necessary to prevent erosion of our collective reasonable expectations of privacy.

---

* Joe Vacek is a tenured associate professor at the University of North Dakota School of Aerospace Sciences. He teaches aviation and space law, transportation, environmental policy, and aviation technical classes at the undergraduate, honors, and graduate levels. Vacek's primary research area is the law of remote sensing, both international and domestic; he focuses specifically on Fourth Amendment search and seizure, privacy, and civil issues related to manned and unmanned aircraft systems and space-based systems. He holds commercial pilot and certified flight instructor certificates, is a practicing lawyer and mediator, and is a former Peace Corps volunteer. He is also the faculty advisor for the UND competition aerobatic flying team. Outside of academia, Vacek enjoys endurance sports, having recently completed an Ironman triathlon, swum a marathon, and ridden his bicycle across the United States. He commutes by bicycle year round in his hometown of Grand Forks, North Dakota.

I. INTRODUCTION

The flight of Unmanned Aircraft Systems ("UAS"), or Drones, in the national airspace has become an ordinary, unremarkable event. Neither the technology for remotely controlled or even autonomous flight nor the aerodynamics of fixed wing or helicopter-type drones are new, having been developed and operational in various forms since World War II. Since that time, a cottage industry of remote-controlled aircraft enthusiasts and hobbyists has existed, mostly for the pleasure of constructing and flying scale-model aircraft at local parks. Remote sensing technology in the United States developed along a similar timeline, with World War II and the Cold War prompting research and development of relatively lightweight and small airborne cameras and sensing equipment, which also spurred development of a cottage industry of amateur photo and video enthusiasts.

Together, these ingredients now provide cheap airborne imaging equipment available to the general public in the United States. Currently, amateur civilian drone operators may remotely sense persons and property practically without limitation. Commercial drone operators have obtained special permission and are eagerly awaiting the publication of proposed rules allowing widespread use of drones for remote sensing. And existing precedent allows warrantless airborne remote sensing by police of private

areas in open view from a legal altitude[1] using technology in general public use[2] as long as the remote sensing does not penetrate into a home.[3] The common law and the proposed rules will likely follow suit, and operating a drone to photograph people from above in a manner that complies with applicable federal aviation regulations will probably not give rise to a civil suit for invasion of privacy or trespass. Operation of the drone itself is only the first step, however. The remote sensing, use, and storage of the data are all open questions under current laws, and protection of that data is problematic because of a fragmentary legal structure.

This article will examine in detail the existing legal structure governing airborne remote sensing by drone in three sections. First, it will canvas applicable principles of common law and existing federal regulations and statutes. Second, it will explore constitutional issues pertinent to government and police remote sensing using drones. Third, it will move to an analysis of current civil use and misuse of drones by the general public. It concludes by arguing that the existing data protection laws in the United States are wholly inadequate to protect citizens' remotely sensed data from unauthorized government or private use. In combination with the widespread availability of small, inexpensive, and automated drones and the widely acknowledged inability of the Federal Aviation Administration ("FAA") to enforce its rules, the implication is that the citizens have nullified the existing rules and laws, such that a significant reduction in subjective and objective reasonable expectations of privacy is inevitable.

II. LAWS REGULATING REMOTE SENSING BY DRONES

The various laws regulating remote sensing by drones developed independently in two different areas of law. The first area is under the framework of tort law, from which the general right of privacy developed in the common law. The second area is under international treaty. Specifically, Article 8 of the Convention on International Civil Aviation from 1944 (the Chicago Treaty) stipulates that "[n]o aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting state without special authorization by that state and in accordance with the terms of such authorization . . . ."[4]

---

1 *See* Florida v. Riley, 488 U.S. 445 (1989); Dow Chem. Co. v. United States, 476 U.S. 227 (1986); California v. Ciraolo, 476 U.S. 207 (1986).

2 Kyllo v. United States, 533 U.S. 27, 27 (2001).

3 Joseph J. Vacek, *Big Brother Will Soon Be Watching—Or Will He?*, 85 N.D. L. REV. 673, 680 (2009).

4. Chicago Convention on International Civil Aviation, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

Tort law has traditionally defined the right of privacy as the right of a person to be free from intrusion upon seclusion, from being shown in a false light, from private information being publicly disclosed, and from misappropriation of his or her likeness.[5] Of course, a person may elect to disclose ordinarily personal or private things in a public forum, such as by posting a revealing Facebook status update or by uploading a compromising photo on Flickr or Pinterest. This behavior is a license for public observation and analogous to the principle that a bell cannot be unrung. Such actions led to the development of the Third-Party Doctrine, which will be explored further later. Overall, though, the common law does not keep pace with technological developments as evidenced by legislators filling gaps with statutory law. But the sensing of private data by drone is a unique case that allows access around many of the barriers erected by the common law and statutory protections, which thus requires singular consideration.

A. FEW LEGAL PRINCIPLES PROTECT REMOTELY SENSED PRIVATE DATA

The legal right to keep certain things private has been imported by the English common law in cases dating back to the early 1800s,[6] specifically for issues concerning intellectual property[7] and photographic images.[8] American common law has also adopted these principles with the development of tort law in the areas of nuisance, invasion of privacy, and trespass, especially. "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[9] And that right, in all cases, belongs solely to the individual in terms of whether or how to grant it to the public.[10] The justification for that right, however, has traditionally been illustrated using the physical process of letter writing and the securing of that single copy of the letter in a locked desk or sealed in an envelope and placed in the mail for delivery. The utility of that analogy arguably has ended with the advent of electronic communications, practically infinite storage and retrieval capability, and airborne remote sensors mounted on

5. *See* RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW INST. 1977).
6. *See, e.g.*, Abernethy v. Hutchinson, 3 L.J. Ch. 209 (1825).
7. *Id.*
8. Pollard v. Photographic Co., 40 Ch. Div. 345 (1888).
9. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).
10. *Id.*

drones. So torts grounded in that theory have only tenuous applicability to privacy invasions or remote sensing via drone.

1. *Common Law Principles of Nuisance, Trespass, and Invasion of Privacy Give Limited Protection from Airborne Remote Sensing*

Common law recognizes several actions in tort that are designed to allow an individual to maintain a privacy wall—literal and metaphorical—between what he or she wishes to keep private and others whose curiosity compels them to snoop. However, physical walls or written letters sealed in paper envelopes bear little relevance to data collection by drone. The three classic tort actions relevant to airborne snooping are the torts of nuisance, trespass, and invasion of privacy. Nuisance is the oldest and broadest of the three and developed in accordance with the legal theory that not only should injuries to the person be compensable, but also injuries to a person's property.[11] The law of nuisance produced the concept of zoning as a preemptive rule to avoid continuous litigation, and the current system of airspace classification in the United States follows similar principles of "zoning" where certain kinds of operations are prohibited in certain classes of airspace. But aside from that nice analogy, the law of nuisance has been described as an "impenetrable jungle . . . [meaning] all things to all people, and has been applied indiscriminately to everything from an alarming advertisement to a cockroach baked in a pie. There is general agreement that it is incapable of any exact or comprehensive definition."[12] Unfortunately, then, in the context of drone operations, there probably exists a set of facts that, when applied creatively to the theory of nuisance, may give rise to injunction or damages against the drone operator. But the way there is not clear.

Trespass, the second classic tort relevant to drone operations, is much more clearly defined in the common law and is bifurcated into trespass to land and trespass to chattels. Trespass to land is defined as a "wrongful interference with another's possessory rights in real property."[13] Possessory rights in real property extend upwards into the airspace to the highest level the possessor can reasonably use[14]—providing a potential cause of action

11. BLACK'S LAW DICTIONARY (9th ed. 2009).

12. WILLIAM LLOYD PROSSER ET AL., PROSSER AND KEETON ON TORTS § 86, 616 (5th ed. 1984).

13. *See, e.g.*, Robert's River Rides, Inc. v. Steamboat Dev. Corp., 520 N.W.2d 294, 301 (Iowa 1994).

14. *See* United States v. Causby, 328 U.S. 256, 260-61 (1946) ("It is ancient doctrine that at common law ownership of the land extended to the periphery of the universe—Cujus est solum ejus est usque ad coelum. But that doctrine has no place in the modern world.").

against drone operators intruding into superadjacent airspace above a plaintiff's land. Much remote sensing equipment is powerful enough, though, to allow an airborne snoop to fly above such superadjacent airspace and avoid a trespass claim.

The other trespass action—trespass to chattels—may possibly provide limited relief. Trespass to chattels has been defined as "an intentional interference with the possession of personal property . . . proximately caus[ing] injury."[15] If the drone operator remotely senses something that could be objectively defined as personal property, a cause of action may arise. A simple example of that could be a photograph taken by drone of a sunbathing person when the person has taken precautions to install a privacy fence to prevent such photography. A more sophisticated example could be the use of a drone programmed to follow a person, remotely sensing that person's location and activities at various times throughout the day, correlating that data with location information, and the subsequent selling of that information to commercial entities for marketing purposes. Following *CompuServe Inc. v. Cyber Promotions*, *Inc.*,[16] the tort of trespass to land could be used to enjoin the kind of remote sensing that could be described as robot paparazzi. Of course, physically being in public weighs against civil privacy rights, but the law recognizes a distinction between privacy rights of public figures versus those of ordinary citizens,[17] and that distinction would appear to apply here as well.

Finally, the relatively new tort action of invasion of privacy may provide a potential cause of action in the context of snooping drones.[18] The right to privacy arises under the traditional civil tort action of intrusion upon seclusion.[19] While state court rulings vary under this theory, the tort is generally viewed to have originated from a Harvard Law Review article authored by Samuel Warren and Louis Brandeis in 1890. Cognizant that technology would develop faster than the law, they foreshadowed the need for legal protection from prying eyes: "[N]ow that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation."[20] Brandeis and Warren clearly foresaw

15. Thrifty-Tel, Inc., v. Bezenek, 46 Cal. Rptr. 2d 468, 473 (Ct. App. 1996).

16. 962 F. Supp. 1015 (S.D. Ohio 1997). Here the court applied the principles of trespass to chattels to support its holding enjoining unsolicited bulk e-mail from being sent. *Id.* at 1021.

17. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 281 (1964) ("The public benefit from publicity is so great and the chance of injury to private character so small that such discussion [regarding public figures] must be privileged.").

18. Allstate Ins. Co. v. Ginsberg, 351 F.3d 473, 480 (11th Cir. 2003).

19. *See id.*

20. Warren & Brandeis, *supra* note 9, at 210-21.

the potential erosion of personal privacy in the face of technologically assisted prying eyes and ears and advocated for the creation of a specific right to privacy, constructing their theory from the areas of intentional torts against the person, nuisance, and intellectual property.[21] From those, the argument follows that "the principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy . . . ."[22] Legal scholar William Prosser elaborated upon the foundations of Brandeis and Warren in a law review article in 1960[23] where he argued that the right to privacy had been legally established in four separate but related areas: intrusion, public disclosure, false light, and appropriation. Prosser noted that cases showed these related legal principles "have been supported by genuine public demand and lively public feeling, and made necessary by real abuses on the part of defendants who have brought it all upon themselves."[24] Similar public demand, lively debate, and the potential for abuse point towards the continued relevance of expanding the privacy torts to remotely sensed private data.

2. *The Third-Party Doctrine Precludes Meaningful Control Over Most Remotely Sensed Private Data*

The Third-Party Doctrine is a legal theory relevant to remotely sensed private data used by government agencies or police. While it has not been applied to private parties involved in a tort action,[25] the doctrine's underpinnings closely parallel the civil right to privacy discussed earlier. The Third-Party Doctrine from *Smith v. Maryland*[26] essentially holds that individuals who disclose private information to third parties have no reasonable expectation of privacy in that disclosed data.[27] *Smith* is the "pen register" case where the Supreme Court held that while the contents of the conversation may be protected, the information voluntarily provided to a third party, the numbers dialed by the defendant, was not.[28] Congress responded with the Pen Register Act, which requires a search warrant for obtaining evidence via pen register.[29]

---

21. *Id.* at 213.
22. *Id.*
23. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
24. *Id.* at 423.
25. The current cases that comprise the "third-party doctrine" all arise from criminal matters. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).
26. 442 U.S. 735 (1979).
27. *Id.* at 744-45.
28. *Id.* at 774.
29. 18 U.S.C. § 3121(a) (2006).

But aside from pen register situations, commentators[30] have demonstrated that the protections individuals have in their private data is quite limited and inconsistent—that "information that has been exposed to middlemen, from medical and financial data to our reading habits"[31] is without Fourth Amendment protection. In fact, the Court has constructed a special category of information described as "transactional" data[32]—which is essentially metadata[33]—the "outsides" of data packets. This metadata is literally the outside of a physical envelope or the numbers dialed on a phone or the GPS coordinates from which protected data is transmitted. The problem is that the metadata is sometimes as rich, or even richer, in content than the constitutionally protected data it describes,[34] which can be incredibly valuable as evidence. Harvesting metadata is relatively simple; a small drone equipped with an appropriately tuned radio frequency scanner[35] can select and record all transmissions within line-of-sight. And the "sight radius" of a small drone operating at a few hundred feet is several orders of magnitude larger than a ground-based unit.

The Sixth Circuit bolstered the Third-Party Doctrine in the context of remote sensing by drone in *United States v. Skinner*.[36] In *Skinner*, the court held that warrantless tracking of the defendant by use of his mobile phone location data was not unreasonable because he had no "reasonable expectation of privacy in the data given off" by his phone.[37] That case appears to clear the way for metadata harvesting by drone, although various federal statutes and regulations may still protect the content of a wirelessly transmitted communication.

30. *See, e.g.*, Jay Stanley, *The Crisis in Fourth Amendment Jurisprudence*, AM. CONST. SOC'Y (2010), https://www.acslaw.org/files/ACS%20Issue%20Brief%20%20Stanley%204th%20Amendment.pdf.

31. *Id.* at 4.

32. *Id.*

33. Metadata is data that describes other data, which includes structural information and descriptive information.

34. An example of rich metadata could be the GPS coordinates from where a series of cryptic text messages were sent and received, followed by the GPS location of where the transmitting device (and suspect) then traveled.

35. An example of such a device is a Cellebrite Universal Forensic Extraction Device, which, among other capabilities, can harvest and record data transmissions from cellular devices and smartphones.

36. 690 F.3d 772 (6th Cir. 2012).

37. *Id.* at 777.

B. FEDERAL STATUTES AND AVIATION REGULATIONS GENERALLY PERMIT REMOTE SENSING

There are a few federal statutes that may potentially regulate remotely sensed data by drone, and several existing and proposed Federal Aviation Regulations ("FARs") directly apply to drone operations, but together they provide little protection from, control over, or remedy for abuse of remotely sensed data by drone. The relevant federal statutes are the Wiretap Act,[38] the Stored Communications Act,[39] and the Pen Register Act,[40] which are all part of the Electronic Communications Protections Act ("ECPA").[41] The applicable FARs include operating rules from 14 CFR 91 and the proposed regulations to be numbered 14 CFR 107.[42]

1. *The Electronic Communications Privacy Act Allows Practically Unfettered Data Gathering Via Drone*

While the ECPA generally prohibits the interception and use of the contents of electronic communications,[43] the potentially evidence-rich metadata that describes those communications and is used to identify, sort, store, and deliver the communication via the internet has virtually no protection. "Electronic communications means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ."[44] As the discussion of the Third-Party Doctrine above[45] indicates, drones make ideal platforms for remotely sensing data transmitted wirelessly, as well as for direct sensing of the ground or subjects below via optical camera or otherwise. Interception of a wirelessly transmitted signal would clearly fall under the definition of "electronic communications" for the purposes of the ECPA, as would a number of other kinds of airborne interceptions. However, there are four exceptions under the ECPA for wire or oral communications, communications made by pager devices (tone-only), communications from tracking devices, and

38. 18 U.S.C. § 2510 (2006).
39. 18 U.S.C. § 2701 (2006).
40. 18 U.S.C. § 3121 (2006).
41. 18 U.S.C. § 2510 (2006).
42. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45).
43. 18 U.S.C. §§ 2511(1)(a)-(e) (2006).
44. 18 U.S.C. § 2510(12) (2012).
45. *See* discussion *supra* Part II.A.2.

electronic funds transfer information.[46] In the drone context, remote sensing of location via tracking devices is probably most relevant. A tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[47] Because sensing location information is thusly exempted from protection under the ECPA, and the Sixth Circuit Court of Appeals broadened that notion in *Skinner* to all emanated data, the ECPA itself appears to give very little protection to remotely sensed location data or metadata.

The Wiretap Act,[48] part of the ECPA, prohibits governmental interception of in-transit communications without a search warrant. The key here is that the communications or data must actually be in transit.[49] But aside from voice calls, most electronic communications and data are actually stationary, stored in a server awaiting transmission or another server awaiting retrieval by the recipient versus moving along the network.[50] Thus, it is a very simple thing to avoid violating the Wiretap Act; all authorities must do is avoid intercepting communications or data while it is moving. So, while operation of a drone equipped with a packet analyzer program[51] by a private party or a government actor without a search warrant would violate the Wiretap Act, it does nothing to narrow the large "emanated data" loophole discussed earlier.

Finally, the Stored Communications Act[52] governs electronic communications not in transit—those stored on a computer server. It was enacted to prevent unlawful or unauthorized disclosures of electronic communication while in electronic storage by third-party providers.[53] While at first glance this seems to be a restriction on the Third-Party Doctrine that protects data from snooping when it is not in transit (which is most of the time), it still only protects the "physical contents" of the data, not the metadata. For example, an email's message would be protected when stored on a server, but not the to/from headers, which are considered to be "outside the envelope" and thus would fall under the purview of the Wiretap Act. Additionally, there is uncertainty as to the status of old, archived communications, such as archived email, which may have less

46. 18 U.S.C. § 2510(12) (2012).
47. 18 U.S.C. § 3117(b) (2006).
48. 18 U.S.C. § 2511 (2006).
49. *Id.*
50. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 981-82 (C.D. Cal. 2010).
51. A packet analyzer is a computer program that can intercept and record data traveling through a network. As data moves through the network, the analyzer can capture a packet, decode the packet's raw data, including metadata, and analyze its content.
52. 18 U.S.C. §§ 2701-2712 (2006).
53. 18 U.S.C. § 2701 (2006).

protection under the Stored Communication Act.[54] For a drone that has been assigned a mission to orbit and "listen" for metadata and location information being emanated or transmitted wirelessly, none of the parts of the ECPA just described would protect that metadata or location information.

2. *Current and Proposed Federal Aviation Regulations Generally Allow Remote Sensing by Drones*

The FAA currently prohibits the commercial use of small drones without special prior authorization,[55] but that prohibition has been challenged in at least one case[56] and is widely viewed as ineffective.[57] Current federal aviation regulations are silent regarding drones or unmanned aircraft, but the Agency has recently proposed a new section to the federal aviation regulations specific to small drone operations.[58] Those newly proposed regulations would apply only to commercial operations, however, leaving civilian amateur enthusiasts and hobbyists as they currently are, which is essentially free to use their small crafts for remote sensing so long as they follow the guidelines for amateur model aircraft operators,[59] and such guidelines are generally limited to avoiding flying over crowds of people or otherwise endangering them and avoiding airports and aircraft operations. Those amateur-operator guidelines are silent as to whether or not a model aircraft may be equipped with a camera or other remote-sensing equipment.

Governmental entities currently may operate a small drone equipped with a remote sensor by way of obtaining a Certificate of Authorization ("COA"), which is a regulatory waiver that allows relatively limited, non-commercial operations.[60] More discussion of regulatory and other limitations on government use of drones follows later. However, in both

54. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

55. FED. AVIATION ADMIN., INTERIM OPERATIONAL APPROVAL GUIDANCE 08-01: UNMANNED AIRCRAFT SYSTEMS OPERATIONS IN U.S. NAT'L AIRSPACE SYSTEM 4 (Mar. 13, 2008), *available at* http://www faa.gov/about/officeorg/headquartersoffices/ato/service units/systemops/aaim/organizations/uas/coa/faq/media/uasguidance08-01.pdf.

56. *See, e.g.*, Huerta v. Pirker, NTSB Order No. EA-5730, 2014 WL 8095629 (Nov. 18, 2014).

57. Jack Nicas & Andy Pasztor, *FAA, Drones Clash on Rules for Unmanned Aircraft*, WALL ST. J., May 11, 2014, http://online.wsj.com/news/articles/SB10001424052702303851804579555144292258188.

58. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45).

59. FED. AVIATION ADMIN., *Advisory Circular 91-57* (June 9, 1981), *available at* http://www faa.gov/documentlibrary/media/advisorycircular/91-57.pdf.

60. INTERIM OPERATIONAL APPROVAL GUIDANCE 08-01, *supra* note 55, at 4.

the proposed regulations and in FAA's policy document "Integration of Civil Unmanned Aircraft Systems ("UAS") in the National Airspace ("NAS") Roadmap,"[61] the general issue of privacy related to remote sensing by drone is raised multiple times, but no enforceable regulatory guidance or prohibitions are provided.

3. *The Privacy Act and a Presidential Memorandum Provide Some Limitations on Federal Agencies for the Collection, Retention, and Dissemination of Remotely Sensed Data*

The Privacy Act of 1974 and a Presidential Memorandum remain the last potential legal and policy protections against widespread airborne remote sensing of private data. The Privacy Act[62] regulates federal governmental agency collection, maintenance, use, and dissemination of personally identifiable information about individuals[63] unless one or more of twelve exceptions applies.[64] The exceptions appear to render the Privacy Act relatively toothless for protecting remotely sensed data. Two significant exceptions that serve as examples in the context of drone remote sensing are the exception for law enforcement purposes[65] and the exception for consumer reporting agencies.[66] It appears that data gathered by airborne remote sensing would be treated the same way as any other information subject to the Privacy Act, regardless of the fact that airborne remote sensing facilitates data gathering orders of much greater magnitude than the less sophisticated methods in place when the statute was drafted in 1974.

A Presidential Memorandum titled "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems"[67] was published concurrently with the Notice of Proposed Rulemaking for the proposed federal aviation regulations governing the operation of small drones. A Presidential Memorandum is very similar to an executive order, neither of which has a basis for existence in the Constitution and both of which are a form of executive legislation and have the full force of law if made pursuant

61. FED. AVIATION ADMIN., INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE NATIONAL AIRSPACE (NAS) ROADMAP (2013), *available at* http://www.faa.gov/uas/media/uasroadmap2013.pdf.

62. 5 U.S.C. § 552a (2006).

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. Presidential Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015), *available at* http://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

to a congressional act that delegates some power to the executive. Here, the FAA Modernization and Reform Act of 2012[68] is the required congressional act, which contains a directive to the Secretary of Transportation (an executive appointee) to develop a plan to safely integrate UAS into the national airspace.[69] Therefore, the Memorandum appears to be a legally binding instrument that orders federal agencies to take into account "privacy, civil rights, and civil liberties"[70] concerns related to the operations of drones.

Specifically, the Memorandum establishes guidelines for federal agencies in addition to already existing laws, such as the Privacy Act, to promulgate policies and procedures for protecting privacy, protecting civil rights and civil liberties, accountability, transparency, and reporting.[71] For protection of privacy, "agencies shall, prior to deployment of new UAS technology and at least every 3 years, examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected."[72] A time limit for retention of collected information is set at 180 days, unless longer times are necessary or required.[73] For protection of civil rights and civil liberties, the Memorandum reminds agencies to put in place policies to prohibit violating the First Amendment or other parts of the Constitution.[74] For accountability, the Memorandum requires agencies to establish policies addressing audits, subcontractors, oversight, asset sharing, data use and sharing, and grant funding matters.[75] For transparency, the Memorandum requires agencies inform the public about UAS missions, location, and an annual summary of operations including a brief description and number of operations, but only to the extent such information would not reveal compromising law enforcement or security information.[76] Finally, each agency must provide status reports to the President and public instructions for accessing the policies and procedures implemented by the Memorandum.[77]

68. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11.
69. *Id.*
70. *See* Presidential Memorandum, *supra* note 67, at 1.
71. *Id.* at 1-2.
72. *Id.*
73. *Id.* at 2.
74. *Id.*
75. *Id.*
76. *Id.* at 2-3.
77. *Id.* at 3.

III. GOVERNMENT VERSUS CIVIL USE OF DRONES

The use of remote sensing technology by the government or police against citizens in the United States has traditionally been limited by the warrant requirement of the Fourth Amendment.[78] Such use by police to surveil citizens led to cases questioning the extent to which the government could use remote sensing equipment to monitor citizens. The most famous of those cases is *Katz v. United States*,[79] where the government used a remote sensing device—a microphone—to listen to a private conversation occurring in a public telephone booth without a search warrant.[80] In deciding whether such remote sensing activities were appropriate to use against citizens in public places, the Court focused on the overarching Constitutional principle that "the Fourth Amendment protects people, not places"[81] and treated the technological surveillance methods as secondary. Under *Katz*, regardless of the location or remote sensing method, private data from a conversation is protected from unreasonable search and seizure under the Fourth Amendment if it is made with a reasonable expectation of privacy.[82]

A. THE FOURTH AMENDMENT CONSTRAINS GOVERNMENTAL REMOTE SENSING BY DRONE

The Fourth Amendment states "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[83] In the context of airborne remote sensing, a number of Supreme Court decisions exist that are directly on point. In those cases, the aircraft has been a manned, piloted aircraft, but the distinction is irrelevant for the sensing function of the platform.

78. U.S. CONST. amend. IV.
79. 389 U.S. 347 (1967).
80. *Id.* at 348.
81. *Id.* at 351.
82. *Id.* at 353.
83. U.S. CONST. amend. IV.

1. *Airborne Warrantless Remote Sensing from a Legal Altitude Is Generally Not a Violation of the Fourth Amendment*

Airborne warrantless searches are generally equivalent to an "open fields"[84] search and are usually constitutional if they are of an "area in open view from any legal altitude . . . as long as the technology used to obtain the surveillance is in general public use and does not penetrate into the home."[85] That principle is distilled from four Supreme Court decisions. Three of those—*California v. Ciraolo*,[86] *Florida v. Riley*,[87] and *Dow Chemical Co. v. United States*[88]—are pertinent to the "airborne" part. In *Ciraolo*, police used a small fixed-wing aircraft to observe the defendant's fenced backyard from 1000 feet.[89] In *Riley*, police used a helicopter to observe the interior of the defendant's enclosed greenhouse from a much lower altitude.[90] In *Dow Chemical*, an agency used a fixed-wing aircraft to photograph the corporation's secure facility from above.[91] In all the cases, no search warrant was obtained and the Court found no Fourth Amendment violation. The fourth case sets the bar for the remote sensing part.

About a decade later, the Supreme Court limited the extent police could use sophisticated remote sensing equipment without a search warrant. In *Kyllo v. United States*, police used a thermal imaging device to infer the internal temperature of the defendant's home by observing the infrared signature emitted by the house.[92] The Court held that such penetrating remote sensing searches are unconstitutional without a search warrant,[93] which appears to limit technological erosion of privacy. Additionally, the Court tied part of its reasoning to the availability of the technology to the general public.[94]

Although at the time of the decision thermal imaging devices were quite expensive and not widely available, they have become relatively commonplace now. A more troubling issue is that thermal remote sensing is not a "penetrating" search at all,[95] and much more recent cases indicate

84. Hester v. United States, 265 U.S. 57, 59 (1924).
85. Vacek, *supra* note 3, at 683-84 (citing Kyllo v. United States, 533 U.S. 27, 44 (2001)).
86. 476 U.S. 207 (1986).
87. 488 U.S. 445 (1989).
88. 476 U.S. 227 (1986).
89. 476 U.S. at 209.
90. 488 U.S. at 450.
91. 476 U.S. at 229.
92. 533 U.S. 27, 29 (2001).
93. *Id.* at 40.
94. *Id.* at 34.
95. *Id.* at 40. The technology at issue in *Kyllo* had nothing to do with penetration of a home, such as the justices perhaps imagined akin to x-ray glasses. Instead, the remote sensing equipment

that any emanations of data—be it thermal, electromagnetic, sound, or other—are not protected.

2. *Persistent, Penetrating, or Technologically Sophisticated Remote Sensing Probably Requires a Search Warrant*

Airborne warrantless searches are generally held to be equivalent to an "open fields" search and are usually constitutional if they are of an "area in open view from any legal altitude . . . as long as the technology used to obtain the surveillance is in general public use and does not penetrate into the home."[96] The original *Katz* postulation that "the Fourth Amendment protects people, not places"[97] applied to the *United States v. Jones* allusions to search duration[98] and to several notable cases involving searches by sophisticated remote sensing technology, and it leads to the argument that persistent, penetrating, or technologically sophisticated remote sensing probably requires a search warrant.

In *United States v. Jones*,[99] the Supreme Court decided that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'" under the Fourth Amendment.[100] Much of the opinion focused narrowly on the issue of physical trespass to the defendant's vehicle.[101] Although the theme of time or search duration appeared no less than seventeen times throughout the opinion and concurrences, the Court maintained that its holding did not concern whether the search or the duration of the search was reasonable because the sole question was binary: whether or not a search had occurred. That left open the question of whether similar "remote sensing-type" warrantless searches would be reasonable absent a physical trespass. After the *Jones* decision in 2012, several cases related to remote sensing have been decided that bear on the issue of warrantless remote sensing searches.

---

employed by law enforcement simply sensed a normally invisible part of the electromagnetic spectrum—infrared light, which is just slightly "longer" than red light—imperceptible to human vision. Although shorter wavelengths of electromagnetic energy, such as the type used in x-ray imaging, actually can penetrate obstructions to vision, the *Kyllo* case appears to have had the physics of electromagnetic imaging exactly backwards.

96. Vacek, *supra* note 3, at 683.

97. Katz v. United States, 389 U.S. 347, 351 (1967).

98. 132 S.Ct. 945 (2012). References to search duration or time occurred seventeen times throughout the opinion.

99. *Id.* at 949.

100. *Id.*

101. *Id.*

In *United States v. Skinner*,[102] the Sixth Circuit Court of Appeals held that warrantless tracking of the defendant by use of his mobile phone location data was not unreasonable because he had "no reasonable expectation of privacy in the data given off" by his phone.[103] The duration of the data collection was three days, which the court noted was not "extreme comprehensive tracking," unlike the four weeks of tracking in *Jones*.[104] Also of note was the court's reliance on the lack of "physical intrusion" in its analysis of whether governmental monitoring of the defendant's broadcast data violated the Fourth Amendment and the court's finding that "[u]sing a more efficient means of discovering [defendant's location] does not amount to a Fourth Amendment violation."[105]

Finally, in *Florida v. Jardines*,[106] the Supreme Court held that the warrantless search of defendant's front porch by use of a drug-sniffing dog violated the Fourth Amendment, and a search warrant was required.[107] Throughout the opinion, the Court analogized to remote sensing devices in constructing its holding, referring to thermal imaging devices (like those used in *Kyllo*) and high-powered binoculars.[108] From these recent cases, it appears that the courts are shifting in their analyses of warrantless searching from an outdated focus on physical limitations to an approach more appropriate to the reality of the age of wireless data and unmanned aircraft.

Read together, these cases appear to indicate that the longer the duration of a surveillance situation (especially via drone), the more traditionally "private" the object of surveillance (such as the curtilage or the home), and the more technologically invasive the surveillance methods, the more likely courts will require a search warrant. In the long view, it may be best to follow Justice Potter's observation from his concurrence in *Katz*: the Fourth Amendment "protects people, not places."[109] His wisdom could be applied in a data or information context; the Fourth Amendment should protect information, not the place where it is found.

102. 690 F.3d 772 (6th Cir. 2012).
103. *Id.* at 777.
104. *Id.* at 780.
105. *Id.* at 779.
106. 133 S.Ct. 1409 (2013).
107. *Id.* at 1417-18.
108. *Id.* at 1418 (Kagan, J., concurring).
109. Katz v. United States, 389 U.S. 347, 351 (1967).

B. THERE ARE VIRTUALLY NO CONSTRAINTS ON CIVIL AND COMMERCIAL REMOTE SENSING BY DRONE

Capable, small drones are ubiquitous in the marketplace today, and amateur operators and commercial outfits have taken advantage of their remote sensing capabilities and low prices, such that small drone activities in the United States have literally taken off.[110] Such activities include real estate aerial photography, surface mine mapping, and videography by businesses as large as Nike, BMW, and Wal-Mart.[111] While the Fourth Amendment, various federal laws, and the Presidential Memorandum discussed above limit the federal government and its agencies' remote-sensing activities using drones, no such limitations exist for private civilian actors or commercial entities using drones for remote sensing. The FAA claims it has authority over all airspace at all altitudes in the United States[112] and over all aircraft, defined as "any contrivance invented, used, or designed to navigate, or fly in, the air."[113] But despite that broad authority, non-commercial hobbyists have been historically ignored by FAA in terms of following normal aircraft operating rules and regulations as long as they avoided manned aircraft and airports.[114] And related specifically to remote sensing, the FAA has no legislative authority to promulgate—or even consider—privacy-related issues.

1. *FAA Generally Ignores Private Hobbyist Use of Drones to Conduct Remote Sensing*

Since 1981, the FAA has ignored private operators of model aircraft[115] in terms of operating rules or regulations because model aircraft flight posed little risk to other aircraft or people on the ground. The FAA provided non-mandatory guidance to modelers in an advisory document,[116] which generally advised operators to avoid flying over crowds of people or otherwise endangering them and to avoid airports and aircraft operations.[117] By complying with those guidelines, model aircraft operators avoided

110. *See, e.g.*, Jack Nicas, *Drone Ban? Corporations Skirt Rules*, WALL ST. J., Feb. 19, 2015, http://www.wsj.com/articles/drone-ban-corporations-skirt-rules-1424373939.

111. *Id.*

112. Huerta v. Pirker, NTSB Order No. EA-5730, 2014 WL 8095629 (Nov. 18, 2014).

113. 49 U.S.C. § 40102(a)(6) (2012).

114. *See Advisory Circular*, *supra* note 59 (providing safety guidelines, not regulations, for model aircraft operators).

115. Model aircraft are technologically and aerodynamically identical to modern drones in terms of systems, control, and risk to other aircraft and people on the ground.

116. *See Advisory Circular*, *supra* note 59.

117. *Id.*

having to comply with the comparatively more complex regulations for manned aircraft.

A similar scheme exists in the proposed regulations for small unmanned aircraft in the new FAR part 107. The new regulations would only apply to non-hobby or non-recreational purposes[118] per Section 336 of the FAA Modernization and Reform Act of 2012, which states "the Administrator of the Federal Aviation Administration may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft"[119] as long as it meets several criteria, which are essentially the same requirements in the 1981 advisory circular plus a maximum weight limit of fifty-five pounds.[120] Thus, not only will the FAA continue to ignore private hobbyist use of drones as long they do not impact safety or interfere with other aircraft, they are prohibited by statute from doing so.

2. *The FAA Lacks Jurisdiction over Privacy Issues, Including the Collection, Use, and Dissemination of Remotely Sensed Data*

The FAA has no legislative mandate to consider privacy concerns when determining aircraft operating regulations. Instead, the FAA is tasked with "assigning and maintaining safety as the highest priority in air commerce"[121] while considering a number of other economic or efficiency-type variables.[122] None of the other considerations relate to privacy. Although the Presidential Memorandum discussed above would include the FAA as a federal agency and require the Agency to consider privacy issues and promulgate policy and regulations in accordance with the Memorandum, the FAA generally is not engaged in use of drones, but rather in regulating other persons or entities who are. Thus, the Memorandum directives discussed above do not actually apply to the FAA itself, unless the Agency starts using drones. And if it did, the Memorandum only directs internal agency policy and does not grant the FAA power nor provide direction as to regulations the Agency might promulgate related to privacy or remote sensing.

118. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45).

119. H.R. Rep. No. 112-381, at 68 (2012).

120. *Id.* at 63.

121. 49 U.S.C. § 40101(a)(1) (2012).

122. 49 U.S.C. §§ 40101(a)(2)-(16) (2012).

3. *The National Telecommunications and Information Administration ("NTIA") will Provide Unenforceable Guidance to Commercial Entities on Policies for the Collection, Use, and Dissemination of Remotely Sensed Data*

Lastly, the Memorandum provides:

> Within 90 days of the date of this memorandum, the Department of Commerce, through the National Telecommunications and Information Administration, and in consultation with other interested agencies, will initiate [a] multi-stakeholder engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use.[123]

The NTIA is an executive branch agency tasked with advising the President on telecommunications and information policy issues.[124] Neither the Memorandum nor NTIA's statutory powers provide for any regulatory enforcement process.

IV. CONCLUSION: THE REGULATORY STRUCTURE AND LEGAL REMEDIES CONCERNING COLLECTION, USE, AND DISSEMINATION OF REMOTELY SENSED PRIVATE DATA ARE INSUFFICIENT TO PROTECT REASONABLE EXPECTATIONS OF PRIVACY ABSENT COMPREHENSIVE FEDERAL LEGISLATION

In the context of remote sensing by drone, neither the common law, federal law, nor administrative regulation individually or together provide comprehensive protection of remotely sensed private data. The Fourth Amendment provides some limited protections in the context of government collection of data, but the Third-Party Doctrine significantly limits control of remedies for unauthorized use or dissemination of private data once it has been obtained by a third party. And while persistent, penetrating, or technologically sophisticated remote sensing by government or police is subject to the warrant requirements of the Fourth Amendment, there are no such constraints on civil or commercial remote sensing

123. *See* Memorandum, *supra* note 67, at 3.

124. According to its website:

> NTIA is the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth.

NAT'L TELECOMM. & INFO. AGENCY, *Mission Statement*, http://www ntia.doc.gov/?Wz1=VsHx4Bg0J6b54d2Z.

activities by drone. A single Presidential Memorandum provides some procedural guidance to federal agencies for privacy protection in the context of remote sensing by drone and orders the creation of a multi-stakeholder framework regarding privacy, accountability, and transparency for commercial and private UAS use. The availability of high resolution digital imaging equipment lightweight enough to be mounted on a very small drone allows any person to spy on another in ways much more intrusive than listening over the backyard fence, and the law simply does not adequately contemplate or address the ramifications of that combination. Because states are federally preempted from promulgating aviation regulations, a comprehensive federal legislative enactment would be the most efficient and effective method of limiting both governmental and commercial gathering, use, and dissemination of remotely sensed data by drone.