They Are Watching You: Drones, Data & the Unregulated Commercial Market

Samantha Dorsey *

TABLE OF CONTENTS

* J.D., May 2018, The George Washington University Law School. Member, *Federal Communications Law Journal*, Vols. 69–70.

I. INTRODUCTION

It is a sunny July afternoon and you are laying outside on your pool raft in your fenced-in backyard. You take off your sunglasses to take in the cloudless blue sky—but to your surprise, a small unmanned aircraft system (hereinafter "UAS"), commonly referred to as a drone, is hovering over your backyard. Try yelling at it, try telling the UAS to get off of your property and to stop recording you—see what happens. *Nothing*. The drone is unarmed and is most likely not breaking any law by hovering over your private residence and using its savvy surveillance and data collecting functions.

What information and data were just collected, how much was collected and who collected it? What will happen to the data just collected; will you ever be notified of its use? These are the issues that have arisen in recent years, as the commercial and personal use of UASs have increased, without associated privacy guidelines maintaining the same growth. There is presently no hard-and-fast regulation or law requiring consent before collecting data via UASs, nor any requirement for a UAS operator to notify individuals of their identity or that they will be surveilling their private residences. Thus, a regulatory solution must be implemented to create general guidelines and enforce best practices to limit overreaching UAS data collection.

The present privacy protection framework surrounding the emerging commercial drone market fails to both hold commercial drone operators accountable for data collection and provide individuals with the ability to know what type of information is being collected and by whom. While the expectations of one's privacy has changed a great deal as technology continues to grow, this Note will discuss the necessity of a nationally unified regulatory framework that will designate and place restrictions upon data collection, explain how that data may be used, and establish an accountability log that will provide individuals with the opportunity to access their data that is being collected by a commercial UAS entity. To implement this regulatory framework, Congress will need to pass legislation that addresses all data collection privacy concerns and also grants agencies like the Federal Trade Commission ("FTC") the authority to interpret and establish their specific rules.

Before delving into the major issues and lack of regulations regarding UASs in the commercial market, this Note will provide detailed background information on UASs, basic privacy theories, and the privacy risks that may be implicated by UAS use. The following sections will provide comprehensive insight on the present uses and capabilities of UASs, including privacy issues and attempts to solve such concerns. After addressing the threats UASs pose, a regulatory solution will be proposed.

II. FROM THEN UNTIL NOW: A LOOK AT DRONES

A. What is a UAS and What Are Its Capabilities?

An unmanned aircraft system ("UAS"), commonly referred to as a drone, "is an aircraft without a human pilot onboard."[1] Rather, "the UAS is controlled from an operator on the ground."[2] "Small" UASs will be the primary focus of this Note, unless otherwise specified. Under Federal Aviation Administration ("FAA") regulations, a small UAS is an aircraft weighing less than 55 pounds.[3]

There are many intended uses of UASs, resulting from the varying interests of UAS operators and UAS customers. The primary use for many UAS operators is to collect imaging for real estate endeavors, various inspections, agriculture and filmmaking.[4] Additionally, both nationally and internationally, there has been an increase in utilizing UASs for delivery services from both the operator and customer standpoint.[5]

In an attempt to keep up with demands for faster and more efficient delivery services, many individuals and companies view drone delivery as the next best thing. For example, Amazon, one of the largest delivery services in the United States, currently has a trial-run-stage drone delivery service which it claims will be capable of delivering packages to customers in thirty minutes or less.[6] While Amazon plans on launching its drone delivery service in the United States in the near future, it has already tested this service in the United Kingdom.[7] Amazon's drone delivery trial run in the United Kingdom first delivered an Amazon Fire TV and a bag of popcorn to an Amazon subscriber in December 2016. The entire delivery took a total of thirteen minutes from the customer clicking "order" to the items appearing at the customer's doorstep.[8]

While Amazon may be striving to meet its customers' demands for the fastest delivery possible, there are other motives for drone delivery services.

---

1. Unmanned Aircraft Systems, FAA, www.faa.gov/uas/ [https://perma.cc/47XT-9B9E] (last modified Mar. 21, 2017).
2. *Id.*
3. *See id.*
4. *See* Commercial UAS Exemptions By the Numbers, AUVISI, http://www.auvsi.org/advocacy/exemptions70 [https://perma.cc/L2A9-CC7R] (last visited Apr. 11, 2017).
5. *See* Farhad Manjoo, Think Amazon's Drone Delivery Idea is a Gimmick? Think Again, N.Y. TIMES (Aug. 10, 2016), http://www.nytimes.com/2016/08/11/technology/think-amazons-drone-delivery-idea-is-a-gimmick-think-again.html?_r=0 [https://perma.cc/DSB6-YRCG].
6. Matt McFarland, Amazon Makes its First Drone Delivery in the U.K., CNN (Dec. 14, 2016), http://money.cnn.com/2016/12/14/technology/amazon-drone-delivery/ [https://perma.cc/3Z7N-R9JC]. While the trial run delivery was successful in the United Kingdom, the drone's delivery route flies outside a human's line of sight, which is not yet legal in the United States.
7. *See id.*
8. *Id.*

Internationally, Harvard graduate Keller Rinaudo, has launched *Zipline*, a time-sensitive medical delivery service.[9] *Zipline* drone delivery is more than delivering a television to an impatient customer, it is a new medical advancement that may be used to save lives.

1. Who Can Operate a UAS?

Who is the operator on the ground? As per Part 107 of the FAA's Small Unmanned Aircraft Rule ("Part 107") the operator of a small UAS must be (1) at least 16 years old, (2) have a remote pilot certificate with a small UAS rating, or (3) be directly supervised by someone with such a certificate.[10] In order to qualify for a remote pilot certificate, an individual must either pass an initial aeronautical knowledge test at an FAA-approved knowledge testing center or have an existing non-student Part 61 pilot certificate.[11]

The operators of UASs are required to follow the FAA's newly enacted August 2016, Part 107 Rule, which set forth the new pilot certification and training rules, as well as safety rules including time, height, and speed restrictions for small UASs.[12] These safety regulations may be waived if the FAA authorizes a Section 333 exemption. This is where the problem of data collection begins.[13]

Under the Section 333 exemption, the seemingly most important flying restrictions dictated by Part 107 that provided some privacy protection against nonconsensual data collection (e.g. prohibitions against flying beyond line of sight, over people, at night, and above 400 feet in the air) are not enforced.[14] If a pilot's Section 333 waiver is granted, s/he may operate at night, beyond line of sight, above 400 feet, as well as in other specific types of operation.[15] The exemption is granted when the activity proposed requires such an exemption, like surveying a residential area.[16] This waiver opens up the door to the hypothetical scenario presented in the introduction—the UAS pilot is now authorized to fly or hover above your property, even if you are not a part of the UAS operation.[17] The FAA has set forth very specific safety rules and restrictions to prevent physical collisions or potential security threats (it is

9. *See* April Glaser, Zipline's Keller Rinaudo Explains Why Drone Delivery Took Flight in Rwanda Before the U.S., RECODE (Nov. 11, 2016), http://www.recode.net/2016/11/11/13598806/founder-zipline-drone-delivery-flight-rwanda-blood-keller-rinaudo [https://perma.cc/P5M3-WENU].
10. *See* Unmanned Aircraft Systems, *supra* note 1.
11. *See id.*
12. *See id.*
13. *See id.*
14. *See id.*
15. *See id.*
16. *See id.*
17. *See id.*

illegal to fly, for instance, in Washington D.C. or near airports) but has failed to consider or adopt privacy regulations in its new Part 107 regulation.[18]

2. UAS Surveillance Capabilities

While all UASs have varying levels of surveillance capabilities, many of them are highly advanced. This section will illustrate the level of technology that some UASs possess and how other companies have used similar technology for other means of surveillance and data collection that have led to similar privacy issues.

Many UASs are technologically capable of data collection, and some to a much higher degree than others. Most UASs are "equipped with sophisticated imaging technology that provides the ability to obtain detailed photographs of terrain, people, homes, and even small objects."[19] The giga-pixel cameras used to outfit UASs can "provide real-time video streams at a rate of 10 frames a second" and "track up to 65 different targets across a distance of 65 square miles." They "may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers."[20] The technologies utilized by UASs are growing rapidly, and soon may even include facial recognition.[21] The use and emergence of these technologies will only continue to provide UAS operators with greater tools and capabilities in collecting data.

Similar sensors and surveillance tools used in UASs have already been employed by the likes of Google in its *Google Street View* mapping project, which takes 360 degree views of streets all over the world by way of highly equipped vehicles.[22] Google has since faced privacy-based complaints, as people are concerned with their faces not being properly blurred when the street shots are available on Google's mapping site.[23] However, Google has technically not violated any privacy laws in the United States because under current tort "invasion of privacy" laws, there is no expectation of privacy when a person is in a public space and in fact, the risk of surveillance is assumed.[24]

---

18. *See* Naomi Lachance, D.C.'s No-Drone Zone Gets Help From Superman And E.T., NPR (Mar. 28, 2016), http://www.npr.org/sections/alltechconsidered/2016/03/28/472138137/d-c-s-no-drone-zone-gets-help-from-superman-and-e-t) [https://perma.cc/GZ4Q-AWJL].

19. Domestic Unmanned Aerial Vehicles (UAVs) and Drones, EPIC, https://epic.org/privacy/drones/ [https://perma.cc/SG5S-S2RZ] (last visited Feb. 23, 2018).

20. *Id.*

21. *Id.*

22. Lindsey A. Strachan, Re-Mapping Privacy Law: How the Google Maps Scandal Requires Tort Law Reform, 17 RICH. J.L. & TECH. 1, 1 (2011).

23. *See id.* at 4.

24. *See id.* at 17.

3. Ways in Which UAS Surveillance Data Has Raised Privacy Concerns

You were wearing a yellow shirt and blue jeans outside of the Walmart in your town *someday* since the *Google Street View* initiative took off. Want to know how the world knows that? It is on the Internet. While this simple tidbit of information may not immediately scream "privacy threat!" it certainly may in other circumstances.

Google has maintained that its *Street View* technology is no more revealing than what is already public—and only takes pictures of things so highly public that there is no privacy right to begin with.[25] For example, if someone was photographed by *Street View* technology walking into a pornographic video store, this would not be an invasion of privacy—even though it would likely cause great embarrassment if posted on the Internet for anyone to access.[26] However, Google did begin to blur all faces of individuals captured in street views since mid-2008 after many of these types of concerns and complaints were raised.[27]

When discussing privacy law, it is important to distinguish between public space privacy expectations and private space privacy expectations. While Google may be permitted to take and post public street views, it may face issues when dealing with privately-owned streets. For example, cities like North Oaks, Minnesota requested to have their privately-owned streets' "street views" taken down.[28] These requests were honored by Google because unlike the majority of *Street View* photos of streets and homes, these North Oaks pictures were not initially taken on a publicly owned sidewalk or other publicly-owned parcel of property.[29]

In addition to private property privacy concerns, Google's *Street View* project has had some national security implications. In 2008, *Google Street View* was delayed in the Baltimore and Washington, D.C. area because the Department of Homeland Security was concerned that some of the images may have been taken in security-sensitive locations.[30] Additionally, in that same year, the Department of Defense requested Google not publish *Street View* content of U.S. military bases and remove all existing content of bases.[31] Google complied.[32]

As discussed in this Note's introduction section, on the surface, UASs' initiatives may seem to be free of any menace, but there are still underlying privacy concerns.[33] First, while the primary intention of UAS pilots and/or the companies they represent may be in furtherance of the aforementioned

25. *See id.*
26. *See id.*
27. *See id.* at 7-8.
28. *See id.*
29. *See id.* at 12.
30. *See id.*
31. *See id.*
32. *See id.*
33. Unmanned Aircraft Systems, *supra* note 1 at 2, Sec 1.

uses, the aircraft is still actively surveying the land beneath it and collecting data. Second, the primary intention of the UAS pilot may *only* be to collect data.

B. Privacy and Data Collection

Claims of invasion of privacy often turn on whether the purported victim actually had a reasonable expectation of privacy under the circumstances.[34] This reasonable expectation of privacy has changed as technology has emerged over the past few decades. Surveillance may also be evaluated differently if it occurs in a fleeting instance rather than over a sustained period of time and if there is an understanding of what may become of the collected information.

Privacy and property rights in the modern age are ever-evolving with technological advances and constant data collection. The most pertinent privacy interest implicated by the use of UASs is the "collection of information about people," called "surveillance."[35] "Surveillance takes place in nearly all [UAS] flights, as one of their major purposes is to collect information."[36] Such surveillance may entail a "broad and indiscriminate recording of people on the ground using a camera sensor on the aircraft."[37] It is pertinent to discuss and evaluate all aspects of privacy law and theory to have a strong foundation when approaching the privacy implications of UASs.

1. Reasonable Expectation of Privacy

What is the standard for determining what should be deemed private? Should a homeowner's backyard and home be viewed as private? Since the holding in *United States v. Causby*, the Supreme Court has long held that, "if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere."[38] While the Court in *Causby* was focused on trespass and takings issues, the same rationale may be applied in terms of UAS surveillance over one's land.[39] Moreover, since *Causby*, the Supreme Court has also held that the test for privacy should be based upon what a reasonable person would expect to be private.[40] Should the hypothetical sunbathing landowner expect to have full enjoyment and privacy over his land? The answer to that question is based on what a reasonable person would expect to be private when taking into account both the *Causby* and *Katz* holdings.

---

34. Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

35. *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43965, DOMESTIC DRONES AND PRIVACY: A PRIMER 6 (2015), https://fas.org/sgp/crs/misc/R43965.pdf [https://perma.cc/AK9B-VP7T].

36. *See id.*

37. *See id.*

38. *See* United States v. Causby, 328 U.S. 256, 264 (1946).

39. *See id.* at 267.

40. *See* Katz, 389 U.S. at 347.

While it may be true that an individual going outside in public view would expect to be visible from an aerial aircraft, that is not to say that an individual expects to be recorded or surveyed, especially while on one's own land. While the Fourth Amendment is applicable only to government action, the privacy protection and intrusion standard established in *Katz v. United* States—requiring a person to exhibit an actual expectation of privacy and, that the expectation was reasonable—may reasonably presume that unsolicited surveillance and data collection of an individual on his personal property may constitute an unreasonable intrusion of privacy.[41]

2. Different Types of Surveillance: Pattern of Life

Society's expectations of privacy still exist even with the emergence of technology and data collection. There are two major classifications of surveillance that are helpful to keep in mind when trying to adapt a UAS and its surveillance tactics to that of traditional surveillance. Assuming *arguendo* that a UAS was only surveying over one's land for a fleeting moment, would this reasonably pass the "privacy intrusion" standard? On its face, the answer may appear to be yes, but in reality it likely would not. This question leads us to distinguish between two types of video surveillance and monitoring, "episodic surveillance" and "persistent surveillance," which ultimately yield the same results and may be either intentional or unintentional data collection.[42]

Episodic surveillance is comparable to a snapshot—a UAS flying over one's land and taking, for instance, one short video or picture of the land and then exiting the air space above the property.[43] Alternatively, while persistent surveillance varies in quantitative measures of time and amount of collection, it may be defined as a continuous hovering over an area for a given amount of time as a means of data collection.[44] The issue here is that there is no bright line between episodic and persistent surveillance.

Episodic surveillance, or "incremental observations" may not be seen individually as intrusions of privacy, but when viewed as a whole, the sum total of such data collection may very well be seen as a reasonable violation of privacy.[45] The sum total of the data collection is referred to as a "pattern of life," so while any single still-frame of either of the aforementioned types of surveillance may be in itself a defensible incursion on privacy, the whole video is something more than the sum of its parts.[46]

Although it is not the primary goal of UAS flight, passive data collection occurs through cell phone or computer history tracking in an

41. *See id.*
42. K.K, A Looming Threat, THE ECONOMIST (Mar. 19, 2015), https://www.economist.com/democracy-in-america/2015/03/19/a-looming-threat [https://perma.cc/Q4YS-ZJ6V].
43. *See id.*
44. *See id.*
45. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).
46. *See id.*

episodic and persistent nature.[47] This type of collection persists by way of continuous UAS sensors.[48] Even if the collection is unintentional, it produces a mass of data—without a meaningful opportunity for consent by the individual being surveyed.[49] The difference between passive data collection on a cell phone and on a UAS is that the cell phone user is generally aware that his or her data is being collected and has elected to continue using the cell phone regardless of that invasion.

Therefore, the result of pattern of life data collection, either by passive or impassive intent, allows the UAS pilot, or the pilot's employer, to learn of the intricacies of an individuals' life; including that person's daily habits, relationships, wealth, purchasing preferences, etc. Is this type of surveillance and data collection a reasonable expectation of being in "public?"

3. Data Collection and Post-Collection Uses

Even if one were to say that the initial nonconsensual collection of another individual's data would fail to constitute intrusion of that person's individual privacy interests, "the subsequent manipulation and storage of that data may warrant an alternative privacy analysis."[50] Specifically, the privacy theory of aggregation supposes that while the collection of bits of data, such as episodic data collection, may not violate an individual's privacy interests if left in piece meal form, extensive collection of information from one or multiple sources may rise to the level of a legal privacy intrusion when all information is woven together.[51]

While the privacy theory of aggregation relies upon the compilation of multiple sources, the unique all-encompassing pattern-of-life data collection that emanates from UAS surveillance, in addition to other data collection records (e.g. telephone, banking and/or utility records) only increases the unique privacy infringement beyond the mere collection of those individual data sets.[52]

Furthermore, while some individuals may not be aware of third-party data collection and sharing practices, there is generally a terms and conditions agreement at the beginning of any contract or that appears prior to application use that requires the potential customer or user to consent to their data being collected and the ways in which their data may be used. This element is completely absent in UAS data collection at this time.[53] Thus, an individual may consent to data collection multiple times in a given day—they have given their consent, and they have agreed to having certain data collected—whereas data collection by way of a UAS changes the aggregation theory by

47. *See* Craig Mundie, Privacy Pragmatism: Focus on Data Use, Not Data Collection, 93 FOREIGN AFF. 28, 31 (2014).
48. *See id.*
49. *See id.*
50. THOMPSON II, *supra* note 35, at 8-9.
51. *See* Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 507 (2006).
52. *See id.*
53. *See* id, at 494.

incorporating nonconsensual surveillance to the data compilation unbeknownst to the individual.[54]

In addition to the collection of unauthorized data, data collected by passive means, by, for instance, aerial surveillance for a land development company, has the potential to be sold to third parties.[55] Even though the data was initially collected for one specific use, it may later be used for a different use, to a different party, with different implications for the unknowing individual.[56] What are the results of this data misuse? It could result in a number of scenarios; identity theft or impersonation, personal embarrassment, or even companies making unwarranted or unwelcomed inferences about the individual's preferences or behaviors.[57]

4. Privacy Theories: Control, Autonomy, Anonymity

The use of UASs may not result in an initial categorization of an invasion of privacy in the minds of many, but as this section will discuss, UAS use implicates many of the leading privacy theories. The major tort principles to be prohibited in the realm of privacy law include: (1) intrusion upon the plaintiff's seclusion, solitude, or into his private affairs, (2) public disclosure of embarrassing private facts about the plaintiff, (3) publicity which places the plaintiff in a false light in the public eye, and lastly, (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[58] It is important to note that these privacy laws have not changed in over forty years.[59] These privacy torts were established—yet not updated—with the following privacy theories.

A leading privacy theory is based upon the premise that every individual has the right to control information about oneself, and should retain the ability to decipher to whom and what amount of his or her information should be communicated.[60] This paradigm breaks down when an individual is no longer given the opportunity to consent to the relinquishment of one's data—this will be discussed further in the next subsection concerning aggregation of collected data.[61] The question comes down to how much control should an individual have over how much he or she allows society to see?

Similar to the control theory, the theory of personal autonomy affords an individual the ability to make their own life decisions "free from interference or control by both government and private actors," which nonconsensual UAS drone collection may certainly hinder.[62] The constant

54. *See id.* at 507.
55. Mundie, *supra* note 47 at 526-27.
56. *See id.*
57. *See id.*
58. *See* Strachan, *supra* note 22 at 14.
59. *See id.*
60. *See* ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).
61. *See id.* at Infra section 2C.
62. THOMPSON II, *supra* note 35 at 7 (citing Whalen v. Roe, 429 U.S. 589, 599 (1977)).

threat of having a UAS hovering over one's home could result in self-regulated behavior as a result of the pervasive monitoring that may occur at any given time, which is a far cry from the autonomy that an individual seeks.[63] Self-regulated behavior may be as basic as someone feeling uncomfortable sunbathing in their private backyard. Kenneth Meredith, a Kentucky resident, for example, shot down a drone that was hovering over his backyard while his young daughter was sunbathing and stated, "when you're in your own property, within a six-foot privacy fence, you have the expectation of privacy."[64]

Another privacy theory drawing from the unanswered question of what is "public" is that of anonymity and one's "state of privacy that occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[65] This state of privacy is viewed as being secure when one is within his private residence and land—if this is how anonymity is perceived, then would overhead surveillance of one's own backyard violate this privacy theory?

C. Attempts at Regulating Activity

1. Regulatory Privacy Guidelines

The Electronic Privacy Information Center ("EPIC") petitioned the FAA to establish and enforce privacy rules to protect citizens from such privacy intrusions, but the FAA claimed that privacy issues "[were] beyond the scope of [their] rulemaking."[66] Rather than participate in a public notice and comment rulemaking addressing the issues EPIC wanted to discuss, the FAA teamed up with the Department of Transportation and participated in the National Telecommunications and Information Administration (hereinafter "NTIA") "multi-stakeholder process."[67] This process was "aimed at developing privacy best practices for the commercial and private use of [drones]."[68]

Ultimately however, the FAA did not create any privacy rulemaking or regulatory guidelines, as the NTIA multi-stakeholder process did not produce any legal restrictions on the use of domestic drones for aerial surveillance, nor

63. *See* THOMPSON II, *supra* note 35 at 9.

64. *See* Chris Matyszczyk, Man Shoots Down Drone Hovering Over House, CNET (July 30, 2015), https://www.cnet.com/news/man-shoots-down-drone-hovering-over-house/ [https://perma.cc/5DLX-GHJM].

65. *See* THOMPSON II, *supra* note 35 at 8 (citing WESTIN, *supra* note 60) (internal quotations omitted).

66. *See* EPIC v. FAA—What About Privacy?, DRONEBUSINESS.CENTER (Aug. 24, 2016), https://dronebusiness.center/epic-v-faa-privacy-12046/ [https://perma.cc/Q7MC-QXZM].

67. *See* id; Voluntary Best Practices for UAS Privacy, Transparency, and Accountability, NTIA, https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf [https://perma.cc/4D6L-54DK] (last visited Aug. 30, 2018).

68. *See* EPIC v. FAA—What About Privacy?, *supra* note 66.

establish any legal rights for individuals who are subject to drone surveillance in the United States.[69] Rather, the multi-stakeholder process created nonbinding "best practices" by providing UAS users with recommended privacy guidelines, information for all commercial drone pilots concerning privacy during their pilot certification process, and new guidance to local and state governments on drone privacy issues.[70]

2. State Laws and Concerns

The state of California is known for its beaches, palm trees and Rodeo Drive—all of which attract famous actors, singers, and models. Due to the lack of UAS privacy regulation by the FAA or other federal entities, California Governor Jerry Brown signed a law in 2015 to protect celebrities from paparazzi UASs.[71] The state legislation, in pertinent part, reads that a UAS operator is liable for physical invasion of privacy if that operator "knowingly enters onto the land or into the airspace above the land of another person without permission…in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff."[72]

Wisconsin legislators were concerned with illicit pictures being taken by a UAS and implemented legislation that makes it illegal to photograph a nude image with a drone.[73] The statute reads "whoever uses a drone… with the intent to photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy is guilty of …[a] misdemeanor."[74]

While California and Wisconsin have taken the initiative to establish state-based regulations on the use of UASs, they still have many issues to address concerning data and privacy that may arise from the use of such equipment. Moreover, while these state-based initiatives are steps in the right direction, drones have the capability to fly over more than one state at a time, thus requiring a more nationally-based regulation scheme rather than state-by state-imposed regulations.

---

69. *See id.*; *see also* Voluntary Best Practices for UAS Privacy Transparency and Accountability, *supra* note 67.

70. *See* EPIC v. FAA—What About Privacy?, *supra* note 66; Voluntary Best Practices for UAS Privacy Transparency and Accountability, *supra* note 67.

71. *See* A.B. 856, 2015-2016 Leg., Chapter 521, (Ca. 2015).https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB856 [https://perma.cc/EFR4-4PSG].

72. *See id.*

73. *See* Wisc. State Leg. Act 213 (2014), https://docs.legis.wisconsin.gov/statutes/statutes/942/09/5/b/2/a [https://perma.cc/SV25-E8BP] (creating Crimes Against Reputation, Privacy and Civil Liberties, Chapter 942.10, Use of a Drone).

74. *See id.*

III. ADDRESSING & ANALYZING THE PROBLEM

A. Potential UAS Privacy Infringement Concerns

Privacy expectations are changing as technology continues to grow and emerge at a rapid pace in modern times. Society as a whole may have a new sense of reasonable privacy expectations as popular technologies, like cell phones, computers and their accompanying application systems constantly track users' data. This is not to say that expectations cease to exist in some manner. For instance, individuals may be aware that by using a credit card, their purchase history may be tracked and collected and potentially sold to stores partnering with their credit card company.[75] Online shoppers, or more realistically all Internet users, may know that their search history and interests are being stored and shared through cookies.[76] Users agree to much of this data collection, and users might consider it tolerable because they are willing to give up some of their privacy for the ability to find information in seconds, share their stories and pictures with relatives and friends across the world, and have Amazon TVs and popcorn delivered to their doors at a moment's notice.

In general, it may be that the current rationale held by consumers is that personal data-collection is acceptable as long as the benefits reaped by such technology use is greater than the privacy infringing data collection. While this rationale may not be explicitly agreed upon by society as a whole, it is implicitly what a technology-user agrees to upon using any service that comes with a user agreement. As aforementioned, users often agree to have their data collected and therefore agree to give slight way to their privacy protection.

Users agree to have their data collected because they want to use the technology, or because of necessity. However, it is technically possible to live off of the data collecting grid. If individual users do not want any data collected, they have the option of not using Facebook, Instagram or Snapchat. Users do not have to go online shopping; they may do so in person at a department store using cash—not traceable credit or debit cards. While it would be rather difficult, it is not completely unfeasible for individual users to escape data collection, if they truly wanted to do so.

It seems that the "more good than harm" rationale by consensual data collection users is based on the notion that such users would rather have easy and instantaneous access to family members and news and the ability to order something online that will be delivered in two days without leaving their home. The data collected from consenting users may not be viewed as a negative—and may actually be seen as a beneficial tool for the average

75. Kate Kaye, Mastercard, AMEX Quietly Food Data to Advertisers: Privacy Concerns Prevent Some Targeting Options, ADAGE (Apr. 16, 2013), http://adage.com/article/dataworks/mastercard-amex-feed-data-marketers/240800/ [https://perma.cc/GXK9-GXS3].

76. Chris Hoffman, The May Ways Websites Track You Online, HOW-TO GEEK (Sept. 28, 2016), https://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/ [https://perma.cc/2MB6-CBZC].

technological user. For instance, cookies tracking consensual users online use may lead them to learn of stores that they may not have heard of but sell the goods and provide the same services that they use on a daily basis.[77] For these types of users, the trade-off of having their data collected yields more positive results than being unable to utilize all of the modern advances that are right at their fingertips.

While this "trade-off" agreement between technology operators and technology consumers may work for present technology, it comes up short for potential commercial UAS uses. Even assuming *arguendo* that commercial UAS operators may potentially incorporate data collection agreements with the individuals using their delivery services, this agreement would still fail to address the other non-consenting individuals who may be affected by UAS data collection. While UAS use in the public commercial market is fairly new, the use has not yet reached the level of implied consent where society will just accept the trade-off—because they want these UAS services, they will deal with any and all privacy concerns. Maybe one day, but not now.

Presently, a user-data collection agreement made between, for instance, Facebook and the individual Facebook user who has agreed to have their data collected by Facebook, would be greatly at odds with a UAS operator and a UAS consumer. The disconnect between the parties lies in the UAS operator's ability to collect data from individuals who do not agree to such data collection.[78] The regulations currently in place do not address the lack of consent between UAS operators and individuals who may have data collected, either directly or for aggregate use. It does seem odd that individuals must consent to data collection when simply, and willingly, buying a pair of shoes online, but are not given the choice for opting out of UAS data collection above their homes when they are not even subscribed to such a service.[79]

Moreover, there are numerous potential beneficial uses of commercial UASs, including consumer uses in connection with instantaneous delivery services and medical delivery services, and for businesses in regard to data collection and delivery expansion opportunities.[80] The data collection of non-UASs is primarily based on consensual Internet or credit-based collection; however, privacy from data collection in your own home or backyard is an entirely different type of intrusion of privacy that has not generally been affected by non-consensual technology user agreements—until now.

---

77. *See id.*

78. *See* Solove, *supra* note 51.

79. *See id.*

80. Stephen Shankland, Zipline's Second-Gen Drones Speed its Medical Delivery Business, CNET (Apr. 2, 2018), https://www.cnet.com/news/zipline-new-delivery-drones-fly-medical-supplies-faster-farther/ [https://perma.cc/LV6B-7EQ4]; Anthony Foxx, Growing the Economy through Innovation: New Rules for the Commercial and Scientific Use of Drones, THE WHITE HOUSE: PRESIDENT BARACK OBAMA (June 21, 2016), https://obamawhitehouse.archives.gov/blog/2016/06/21/growing-economy-through-innovation-new-rules-commercial-and-scientific-use-drones [https://perma.cc/3UX8-3GJY].

B. *Current Regulations Are Missing the Mark*

Current regulations are missing the mark in addressing how much, to what extent, and whose data may be collected by way of a UAS. UASs bring up an entirely new aspect of data collection and privacy expectations. UAS operators are no longer just trying to "infringe" on users' online privacy rights but are now capable of collecting data from users'—*and non-users'*—homes and backyards.[81] While the United States' regulations have generally kept up with the times in terms of privacy and privacy expectations on smart phones and computers, the autonomy of ones' privacy within their homes may not have maintained the same adaptation.[82]

Presently, regulations in connection with UASs are primarily concerned with safety regulations and flying ordinances, not with the data collection of UAS operators.[83] As UAS technology grows, the concern must be focused on data collection and individual privacy, as well as safety. While these requirements may be sufficient to ensure that UAS operators are qualified to fly, they fall short of establishing any accountability or transparency in their operations. Presently, under FAA regulations, UAS operators are not required to publicly disclose the data collected during their flights, or what will become of the collected data, nor are they required to obtain consent for such collection from the individuals undergoing surveillance.[84]

IV. A REGULATORY COMPROMISE

While there may be no perfect solution this early in the UAS game, a regulatory framework which will provide best practices and data protection is a respectable starting point. The regulatory framework that I will propose will allow individuals to use UAS delivery services and will protect non-participants. As the use of UASs in the commercial market increases, the framework will likely be amended and nuances will be fleshed out. For now, the most important goal is to give individuals the right to protect their data through clear avenues.

As the drone industry expands, different parties, namely UAS operators and UAS consumers/users, will inevitably seek to have their various interests protected. Therefore, a regulatory framework created and implemented by Congress appears to offer the best solution to balancing data collection and protection of individuals voluntarily using UAS services as well as non-users.

The regulation proposal must address the most pressing issues in UAS data collection and privacy protection to some degree while granting agencies like the FTC and FAA the authority to create detailed means of addressing all concerns. Congress must first address the limitations of UAS consensual user

81. Smartphone Privacy, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 19, 2017), https://www.privacyrights.org/consumer-guides/smartphone-privacy [https://perma.cc/4DCK-HJG4].

82. *See id.*

83. *See* Unmanned Aircraft Systems, *supra* note 1.

84. *See id.*

agreements and create reasonable barriers that allow some data collection but prevent UAS operators from having an unlimited and unwarranted amount of leeway when collecting user data. Additionally, the regulation must address how such collected data is to be controlled in terms of third-party data sharing. Furthermore, the regulation must create boundaries for how much, how long, and what may be collected by UASs passing over non-users' homes for the protection of non-UAS users, who have not agreed to any user agreements and do no personally use any UAS services.

A. Best Practices for Collecting Data from a UAS Delivery Service Customer

This section will consider only delivery service users and will create general limitations for the type of data that may be collected. Data should be collected in an episodic manner and only for purposes of functional use—in other words, data should only be collected for purposes of advertising, generating land maps, or land surveys.

Just as in many other user agreements, the proposed UAS regulation must hold UAS operators accountable for notifying all users of the type of data that can potentially be collected and sold to third parties. While this information may deter some prospective users from using UAS services, it must be made readily available to potential users in the same fashion that the majority of other application systems, retail websites, social media websites or credit card providers inform potential users of the types of data they may collect.[85] Moreover, the UAS operators must be required to distinguish between data being collected in terms of surveillance data, and that of purchasing data—depending on the UAS service being utilized.

For instance, if Amazon's "drone" delivery service ever comes to full fruition in the United States, Amazon would have the ability to collect surveillance data of the Amazon drone delivery subscriber in two ways. First, Amazon would be able to collect data on a subscriber's land size, type of car he or she drives, or how many people live in his or her home, amongst other available data. Second, Amazon would also be able to collect the subscriber's purchasing data and may be able to use that data in its own personal advertisements. Additionally, Amazon has the ability to sell such collected data to affiliated third parties who could potentially use such data in its own aggregate data collection for future solicitation and advertising to that Amazon subscriber.[86]

---

85. Leuan Jolly, Data Protection in the United States: Overview, THOMAS REUTERS PRACTICAL LAW, http://us.practicallaw.com/6-502-0467#a686014 [https://perma.cc/YW9F-5VS4]. The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising and disclose that consumers can opt out of these practices, providing an opt-out mechanism.

86. Kiri Masters, A Simple Guide To Amazon's Complicated Advertising Business, FORBES (June 8, 2018), https://www.forbes.com/sites/kirimasters/2018/06/08/a-simple-guide-to-amazons-complicated-advertising-business/#283aaa623910 [https://perma.cc/M858-JCA6].

Next, in terms of data collection, there must be a balance between the modern "emerging technology and incessant data collection," reasonable expectations of privacy, and simply going too far.[87] If a consumer uses UAS delivery services, they should expect to forego some privacy protections—just like other user agreements that trade service for data. While normal course of business data collection practices should be followed in terms of collecting a subscriber's purchasing history and tendencies, the new regulation should create guidelines for UAS data collection that may take place if the UAS is delivering goods to a home or business.

This type of data collection should be limited to data that can be used for advertising and for corporate use to expand programs and technology based on individuals' likes and dislikes. It should not be used as a tool to exploit or cause reputational harm or embarrassment. While it may seem difficult to view any data collection as not having some type of advertising purpose, there is certainly a limit, even if it may be very broad. Essentially, almost all data can be used for advertising purposes in one way or another, so the regulation here would give agencies the discretion to decide what those limits are and in what way the data may be construed and stored. For instance, it may be acceptable for a UAS to capture a sunbather in her backyard for the purpose of discovering what type of swim brand she is donning, but it may not be permissible to share the actual photo of her in her swimsuit. Here, the regulation should follow the lead from states like California and Wisconsin, who have already imposed data collection limitations to bar pictures of individuals that can be used in any harmful way or used as a tracking device.[88]

The relevant issue is deciding how such permissible data collection should occur via episodic surveillance or persistent surveillance.[89] As previously discussed, regardless of how much data is being collected from seemingly every type of electronic device and application system that an individual interacts with, society's expectation to maintain at least some autonomy in private residences must warrant some regulation of UAS surveillance of private residences.[90]

The reason is that while individuals may have adapted to vast data collection on the Internet and via phone applications with or without their explicit consent, such collection does not literally take place in their own homes, although these technologies are within the user's own home.[91] Thus, it would seem pertinent that the regulation should permit only episodic surveillance of a user's home and only when delivering the goods or

87. *See* United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J. concurring); *See also* Solove, *supra* note 51 at 494.

88. It is important to note the distinction between the California and Wisconsin laws which limit which types of photos may be taken of individuals and the purpose they intend to seek is in stark contrast with Street View whose intention is purely functional. *See* Assembly Bill 856, *supra* note 71; *See* Crimes Against Reputation, Privacy and Civil Liberties, *supra* note 73.

89. *See* Jones, 565 U.S. at 430-31; *see also* Solove, *supra* note 51 at 494.

90. Solove, *supra* note 51 at 90.

91. *See id.*

performing the functions that the user employed the UAS operator to partake in.

As previously addressed, when pieced together, episodic surveillance inevitably and essentially creates the same quantity of data collection as persistent surveillance would.[92] However, the regulation's restriction of allowing only episodic surveillance would more closely resemble the more familiar type of surveillance that could occur by traditional delivery services. Of course, the traditional sense of delivery would yield a less voluminous collection of data than would a UAS's "bird's eye view" advantage but would equate to a more episodic surveillance.

For example, picture a UPS delivery person given the task of both delivering a customer's packages *and* collecting data. The UPS delivery person would not persistently sit outside of the customer's home and take note of all that is visible. Rather, the UPS delivery person would go to the customer's door, deliver the customer's package, take note of the property and any other overt data, and move on to the next delivery. Thus, episodic surveillance closely resembles traditional delivery service and surveillance. While this type of suggested surveillance may incite underlying aggregation theory issues, when put in the UPS delivery person context, the aggregate data collection would still resemble the same kind of data collected on a daily basis by a delivery man.

Moreover, UASs are just yet another type of technology that individuals will inevitably be forced to become accustomed with because it seems evident that they are here to stay—just like the global use of cell phones and computers. Using this logic, the regulation should focus on limiting UAS operators to episodic surveillance because on its face, this surveillance is less intrusive than persistent surveillance. Remember that sunbathing homeowner who was trying to have a nice, relaxing day in a private backyard? While any means of intrusion in one's backyard may be initially be viewed as an intrusion—whether or not it was consented to in a user agreement—it may seem *less* intrusive if the UAS simply flew over the home and did not hover for an extended period of time. Therefore, as a way of allowing individuals to maintain some sense of autonomy and control over what they share with the corporate world, the data collection manner that is *viewed* as (and may actually be) less intrusive is the manner in which the regulation should proceed.

B. Best Practices for Collecting Data from a Non-UAS-Delivery-Services-Participant

While consenting UAS delivery service customers can expect to have more data collected from them to enhance their personalized advertisements, non-participants require protection for their privacy and data collection. The issue is how much is too much data collection? It would be unreasonable and likely impossible to require a UAS operator to be expected to turn on and off its surveillance data collection technology when flying above different homes.

92. *See id.*

While this may very well be a possibility with advanced technology, this Note takes the position that it would be unreasonable to require that these delivery services turn their data collection surveillance off and on when flying above different homes.

The regulatory framework should be two-fold, which will both limit and restrict how collected data is utilized and provide non-participants with opt-out options. As noted earlier, most UAS surveillance obtained from a street view could technically be carried out by other non-UAS means. A UAS could collect data in a more efficient manner, but a person could just as easily sit outside someone's home and obtain the same type of street view data. Thus, it seems impracticable to restrict *all* data collection, so the real protection should lie in the utilization of such collected data.

While data obtained by a publicly accessible view may be collected, it should be restricted in a manner that does not directly link the collected information with the individual surveyed. The data should be anonymized and aggregated to prevent any link between an individual and his or her respective collected data. This may work against employers of UASs because they will not be able to specifically tailor their advertisements to any one individual. However, the issue here is consumer protection, not corporate gain. Again, it is important to note that this anonymous data collection is centrally focused on the notion that it applies only to publicly accessible data.

The next element to the regulatory framework would be creating a "Do-Not-Collect" system where individuals may request that their data not be collected at all, or if it is, to be used in a specific way—whether it be for surveying purposes, advertisement purposes, etc., This system will be tailored to data that is collected beyond the scope of a publicly accessible view. This way, parties are aware that their data is being collected and can make their own autonomous choices. Additionally, this gives the option to consent to data collection if individuals enjoy having a more tailored advertisement experience or just do not care at all.

C. *What About UASs That Are Employed Only for Surveillance—Not Delivery Services?*

As with Google's *Street View* project, UASs are often used for surveillance and mapping.[93] Because privacy laws remained relatively stagnant in the latter part of the twentieth century, there is not much basis for individuals' privacy infringement claims when surveillance photos are taken from public airways into private lots—as long as the images are already readily viewable from a public space.[94]

Moreover, when looking at the "intrusion upon seclusion tort," which has been a principle of tort privacy law since the 1960s, a plaintiff must prove "an intentional intrusion upon the seclusion of their private concerns which was substantial and *highly offensive to a reasonable person*, and aver

93. *See* Domestic Unmanned Aerial Vehicles, *supra* note 19.
94. *See* Strachan, *supra* note 22 at 8, 11.

sufficient facts to establish that the information disclosed would have caused mental suffering, shame or humiliation to a person of ordinary sensibilities."[95] The issue with proving such an intrusion is that it is difficult for a plaintiff to contend that a mere photo of his or her home rises to the level of "highly offensive" conduct to a "reasonable person."[96] Thus, unless the present privacy tort laws are reformed, it would seem logical to follow a similar approach to that of Google's *Street View, by establishing a "take down" request system,* when regulating surveillance of both public and private property.[97]

The regulation should hold that any individual who finds a UAS surveillance-collected image to be intrusive should be given the opportunity to submit an initial formal "take down request" through the company itself. Non-compliant companies would be notified and eventually penalized by the Federal Trade Commission upon refusal to blur or delete the photo through a UAS data collection compliance department. Refusal to comply with individual take down requests would be reviewed and ruled on within the FTC's independent review board, and that would be the final decree unless the complainant chose to appeal to a federal court.

As with the Google *Street View* approach, until privacy tort law is reformed, surveillance that is not highly offensive and is taken from public property is still valid data collection. But society should still be given the opportunity to voice concerns and possibly have images removed from the Internet. Moreover, images that are not explicative or endangering and do not warrant a take down but still contain a person should always be disseminated with the face blurred. This model adapts to modern privacy expectations but still has an interested party, the compliance department, advocating for the prevention of over-indulgent UAS data collection that may violate privacy rights.

V. CONCLUSION

While modern technological emergence relies heavily on data collection, United States privacy laws have failed to keep up with the evolving and growing technical landscape. It has become more and more difficult to draw clear lines as to what constitutes privacy violation in the modern era. The regulations that this Note proposes to keep the newly developing field of commercial UASs in check are the first steps in maintaining accountability of UAS operators and their affiliates. Developing the UAS data collection regulations will provide individuals with the opportunity to engage in the new and exciting technology that UASs encompass while still offering that sun-bathing individual some privacy protection in a world that consistently shrinks the meaning of "reasonable privacy expectations."

95. *Id.* at 14 (quoting Boring v. Google, 362 Fed. App'x 273, 279) (emphasis added).
96. *See id.*
97. *See* id at 13.