FILLING IN THE GAPS IN FAA DRONE REGULATIONS: A PROPOSED DUAL-ZONE MODEL OF PERSONAL PRIVACY

Steve Ragatzki[1]

The current regulations in the United States leave little, if any, recourse for an individual whose privacy has been invaded by another individual using a drone. The proposed drone rules from the Federal Aviation Administration do little to address privacy concerns beyond data security. Further, individual states are adopting wildly different policies that will create a scrambled mess of regulations for drone pilots and citizens alike to sort through. Therefore, a common system of privacy laws should be adopted regarding drone use. The United Kingdom's Protection of Freedoms Act and Data Protection Act and a proposed law by an Australian advocacy group provide a model framework that the states themselves, or the federal government, should impose to ensure individual privacy rights are not trampled in this new age of drones.

I. INTRODUCTION 193
II. THE EXECUTIVE BRANCH HAS ESSENTIALLY PUNTED ON THE ISSUE OF PRIVACY CONCERNS REGARDING DRONES 199
III. THE STATES HAVE ATTEMPTED TO ENACT DRONE PRIVACY LEGISLATION, BUT THEIR EFFORTS ARE MERELY A PATCHWORK SOLUTION TO A BROADER PROBLEM. 206
IV. A MODEL AMERICAN DRONE PRIVACY LAW SHOULD BE BUILT FROM THE FRAMEWORK OF DRONE PRIVACY LAWS FROM THE UNITED KINGDOM AND AUSTRALIA 213
VI. CONCLUSION 231

I. INTRODUCTION

"[A]t root privacy is a simple understanding: not everything belongs to everyone."

---

1. J.D. Candidate, May 2017. Professor Nancy Costello, thank you for your guidance—you always make my writing better. Kyla Barranco, thank you for your love and support throughout the writing process.

— Nick Harkaway, *The Blind Giant*[2]

William Meredith's daughter was sunbathing on July 26, 2015 when she saw the drone flying above her backyard.[3] Although the drone had briefly disappeared when Meredith's daughter waved it off, William Meredith was concerned and grabbed his shotgun.[4] "Within a minute or so, here it [the drone] came. It was hovering over top of my property, and I shot it out of the sky. I didn't shoot across the road, I didn't shoot across my neighbor's fences, I shot directly into the air."[5] Instead of being praised for protecting his privacy rights and preventing someone from spying on his daughter, Meredith was charged with wanton endangerment and criminal mischief.[6] "Our rights are being trampled daily," declared Meredith. "Not on a local level only — but on a state

2. NICK HARKAWAY, THE BLIND GIANT: BEING HUMAN IN A DIGITAL WORLD 122 (2012). This is the premise I will use throughout my article. Many noted scholars—including Justice Douglas of the United States Supreme Court—would potentially disagree. *See* United States v. Causby, 328 U.S. 256 (1946). Justice Douglas, ruling against the owners of a chicken farm that was disrupted by air travel overheard, stated: "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. The air is a public highway, as Congress has declared. Were that not true, every transcontinental flight would subject the operator to countless trespass suits. Common sense revolts at the idea. To recognize such private claims to the airspace would clog these highways, seriously interfere with their control and development in the public interest, and transfer into private ownership that to which only the public has a just claim." *Id.* at 260-261. It is my contention that common sense does not revolt at the idea of restrictions on aircraft above property. Rather, society is in desperate need of some common sense boundaries to stop drones from encroaching on our last remaining spheres of privacy. For a more in-depth discussion of the *United States v. Causby* case, see LAWRENCE LESSING, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

3. Douglas Ernst, *Ky. Man Arrested After Shooting Down $1,800 Drone Hovering Over Sunbathing Daughter*, THE WASH. TIMES (July 30, 2015), http://www.washingtontimes.com/news/2015/jul/30/william-merideth-arrested-after-shooting-down-1800/.

4. *Id.*

5. *Id.*

6. *Id.*

and federal level. We need to have some laws in place to handle these kind of things."[7]

The idea of personal privacy in the United States has been around for over a century.[8] Defining privacy as "the right 'to be let alone,'" Samuel Warren and Louis Brandeis in 1890 proposed an application of existing common laws to protect individuals from instantaneous photographs and the newspaper enterprise.[9] Today, a new encroacher, unmanned aircraft systems (UAS), more commonly known as drones, calls for a similar application of current laws to meet changing privacy concerns in modern society.

The American consumer's appetite for drones is growing rapidly. Some early 2015 reports projected hobbyists in the United States to buy 700,000 drones in 2015, which would represent a 63% increase from the previous year.[10] Officials from the Federal Aviation Administration (FAA) projected that over one million drones were sold in the 2015 holiday season alone.[11] According to Brian Wynne, the CEO for the Association of Unmanned Vehicle Systems International, the drone industry "is poised to be one of the fastest-growing in American history. . . . [D]uring the first decade following [drone] integration . . . , the industry will create more than 100,000 high-paying jobs and provide

---

7. *Id.*

8. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

9. *Id.* at 195.

10. Craig Whitlock, *Federal Regulators to Require Registration of Recreational Drones*, THE WASH. POST (Oct. 19, 2015), https://www.washingtonpost.com/world/national-security/federal-regulators-to-require-registration-of-recreational-drones/2015/10/19/434961be-7664-11e5-a958-d889faf561dc_story.html.

11. Christian de Looper, *The FAA is Very Concerned about the One Million Drones To Be Sold This Holiday Season*, TECH TIMES (Oct. 1, 2015, 4:19 PM), http://www.techtimes.com/articles/90598/20151001/faa-very-concerned-idea-million-drone-sales-holiday-season.htm; Michael del Castillo, *This Christmas 1 Million Expected Drone-Sales Will Need to Include Federal Papers*, N.Y. BUS. J (Oct. 19, 2015, 2:29 PM), http://www.bizjournals.com/newyork/news/2015/10/19/this-christmas-1-million-expected-drone-sales-will.html.

more than $82 billion in positive impact to the nation's economy."[12] This rapid increase in demand for drones ensures that drones will not leave our consciousness, or way of life, anytime soon.

Drones have a wide range of applications for commercial use, "include[ing]: newsgathering; crop and wildlife monitoring; inspections of power lines, pipelines, bridges, and antennas; aerial photography; and other research and educational activities."[13] The FAA recognizes even more potential uses, including aiding in rescue operations.[14]

However, drone operations are not limited to commercial applications. Drones have already been used to spy on women, undressing in high-rise buildings,[15] and sunbathing in their backyard.[16] Private actors are trying to develop solutions for agencies to effectively police drones, but these are not yet ready.[17] In the meantime, consumers are taking privacy protections into their own hands. Items like the DroneDefender, described as "the first portable, accurate, rapid- to-use counter-weapon to stop suspicious or hostile drones in flight, providing critical security protection at home and abroad," allows users to shoot

---

12. *AUVSI Highlights Benefits of Unmanned Aircraft Systems, Need for Small UAS Rule*, AUVSI (Nov. 23, 2015, 3:24 PM), http://www.auvsi.org/blogs/auvsi-membership/2015/11/23/energyandcommerce.

13. Lois Mermelstein, *FAA's New Draft Drone Rules*, 11 THESCITECHLAWYER 14, 14 (2015).

14. Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9543, 9545, 9548 (Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, and 183)[hereinafter Operation of Small Unmanned Aircraft Systems].

15. James Queally, *Seattle Woman Says Drone Seemed to be Spying on Her*, L.A. TIMES (June 24, 2014, 5:31 PM), http://www.latimes.com/nation/nationnow/la-na-nn-seattle-peeping-tom-20140624-story.html.

16. Alex Wellman, *Dad Shoots Down Drone 'Spying on His Sunbathing Daughter' –and is Arrested by Cops*, MIRROR (Aug. 1, 2015, 4:51 PM), http://www.mirror.co.uk/news/
world-news/dad-shoots-down-drone-spying-6177304.

17. Charles E. Ramirez, *Mich Tech Prof Developing Drone to Catch Other Drones*, DETROIT NEWS, (Feb. 15, 2016, 11:36 PM), http://www.detroitnews.com/story/news/local/
michigan/2016/02/15/drone-killer/80435642/.

drones out of the sky in an effort to provide privacy protections for citizens.[18]

The purpose of this note is to demonstrate gaps in the current system of privacy laws in the United States. Although privacy laws exist in each state, individual states have taken wildly disparate actions regarding drones.[19] As a result, a patchwork system of laws leaves great confusion for drone rules around the country. The FAA has also proposed its own drone rules.[20] However, those rules are concerned with administrative matters such as drone registration and collecting pilot information.[21] The FAA even admits that privacy concerns are beyond the scope of its rulemaking.[22]

To combat these inconsistent laws around the country, three things must happen quickly. First, the United States should adopt elements of the United Kingdom's Data Protection Act, and policy recommendations from Australian advocacy group, Liberty Victoria, to provide a clear and consistent set of regulations that will protect individual citizens from new aerial intrusions. Second, the Federal Aviation Administration should enact more stringent registration requirements for all drone operators. To advance the second goal, the Federal Aviation Administration (FAA) must require drone registrants to tag all drones with long-range radio frequency identification devices or some other similar mechanism. Third, a smartphone app should be developed to provide all citizens with a quick and convenient means to identify drones via Radio Frequency

18. Zach Epstein, *New Rifle Shoots Drones out of the Sky Without Firing a Single Bullet,* YAHOO! (Oct. 16, 2015), https://www.yahoo.com/tech/s/rifle-shoots-drones-sky-without-firing-single-bullet-132038513.html.

19. *See infra* Part III.

20. Operation of Small Unmanned Aircraft Systems, *supra* note 14, at 9544.

21. Drone operators must obtain the same airman certificate that pilots of regular aircraft obtain. *Id.* at 9550. Before drones became deregulated for commercial use, operators had to apply for exemptions to the airman certificate requirement under § 333 of the FAA Modernization and Reform Act of 2012. *Id.* at 9552. However, the FAA was more concerned with safety than anything else when granting § 333 exemptions. *Id.* at 9551. The key considerations for the FAA when granting § 333 exemptions are that "(1) the operation must not create a hazard to users of the national airspace system or the public; and (2) the operation must not pose a threat to national security." *Id.* When considering safety, visual line of sight operation is a primary concern. *Id.*

22. *Id.* at 9552.

Identification (RFID). Without a means of long-range identification, any law protecting the personal privacy of a citizen from a drone hovering 400 feet in the air is toothless.[23]

This note is limited to personal privacy concerns only. Criminal procedure privacy concerns surrounding the Fourth Amendment will not be discussed. Those concerns have been thoroughly addressed,[24] and for the purpose of focus over breadth, will not be discussed here. Further, this note will treat all drones — with and without cameras — equally. Citizens whose rights are potentially infringed by a drone flying overhead should not have to determine whether that drone is carrying a camera. To require a citizen to determine whether a drone is carrying a camera before seeking redress for privacy violations is nonsensical when drones can fly hundreds of feet high. Finally, I recognize the inherent limitations of federalism to enact a binding rule upon all states.[25] This note will not discuss the constitutional legitimacy of a federal drone privacy statute, but merely provide a recommendation that the federal government, or all states, should adapt.

With those limitations in mind, this note will propose a new normal for privacy in the United States. Section II will discuss the efforts made by the executive branch of the federal government to define a framework for privacy issues. Section III will examine state efforts to grant drone privacy rights. Finally, Section IV will identify relevant foreign ideas to craft a sweeping drone privacy law for the United States.

---

23. The Federal Aviation Administration has set 400 feet as the maximum height for drone flight. Sarah Gonzalez, *Where Can Drones Fly? Legal Limits are Up in the Air*, NPR (Aug. 10, 2014, 9:43 AM), http://www.npr.org/2014/08/10/339181964/where-can-drones-fly-legal-limits-are-up-in-the-air.

24. *See, e.g.*, Victoria T. San Pedro, *Drone Legislation: Keeping an Eye on Law Enforcement's Latest Surveillance Technology*, 43 STETSON L. REV. 679 (2014); *See also* Y. Douglas Yang, *Big Brother's Grown Wings: The Domestic Proliferation of Drone Surveillance and the Law's Response*, 23 B.U. PUB. INT. L.J. 343 (2014).

25. *See* WELLS C. BENNETT, BROOKINGS INSTITUTION, CIVILIAN DRONES, PRIVACY, AND THE FEDERAL-STATE BALANCE (2014). But there is a possibility that a federal law could "establish a statutory core to be shared by the states, or a statutory floor, permitting state deviation towards more protection." Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIR. 57, 65.

II. THE EXECUTIVE BRANCH HAS ESSENTIALLY PUNTED ON THE ISSUE OF PRIVACY CONCERNS REGARDING DRONES

The delivery truck of the future is not a truck at all — it's a drone.[26] In December 2013, Amazon proposed to deliver packages to customers via autonomous drone delivery.[27] The system, called Prime Air, promises to deliver packages to customers within thirty minutes of an online order.[28] Amazon will use drones weighing more than fifty-five pounds to deliver packages weighing less than five pounds to customers more than ten miles from distribution centers.[29] And this system is not far off. According to Amazon, "[f]rom a technology point of view, we'll be ready to enter commercial operations as soon as the necessary regulations are in place."[30] However, those regulations have proved to be a large hurdle, the biggest challenge to Amazon has been convincing the Federal Aviation Administration (FAA) that drone delivery should be allowed.[31] While Amazon brought the drone issue squarely into the

---

26. Lisa Eadicicco, *Amazon Reveals New Details About Drone Deliveries*, TIME (Jan. 19, 2016), http://time.com/4185117/amazon-prime-air-drone-delivery/.

27. David Streitfeld, *Amazon Floats the Notion of Delivery Drones*, N.Y TIMES: BITS (Dec. 1, 2013, 10:07 PM), http://bits.blogs.nytimes.com/2013/12/01/amazon-floats-the-notion-of-delivery-drones/.

28. *Amazon Prime Air*, AMAZON http://www.amazon.com/b?node=8037720011 (last visited Sept. 26, 2016).

29. David Pogue, *Exclusive: Amazon Reveals Details About Its Crazy Drone Delivery Program*, YAHOO! TECH (Jan. 18, 2016), https://www.yahoo.com/tech/exclusive-amazon-reveals-details-about-134395172543698 2.html.

30. Streitfeld, *supra* note 27.

31. *Id.* The FAA granted Amazon an Experimental Airworthiness Certificate on March 19, 2015. Kelsey D. Atherton, *The FAA Approves Delivery Drones, As Long As Amazon Changes Everything*, POPULAR SCIENCE (Mar. 20, 2015), http://www.popsci.com/faa-approves-delivery-drones-if-amazon-changes-everything. However, the FAA's requirements for testing make Amazon's idea of autonomous drone delivery impossible. *Id.* According to the FAA, "Under the provisions of the certificate, all flight operations must be conducted at 400 feet or below during daylight hours in visual meteorological conditions. The UAS must always remain within visual line-of-sight of the pilot and observer. The pilot actually flying the aircraft must have at least a private pilot's certificate and current medical certification." *Amazon Gets Experimental Airworthiness Certificate*, FEDERAL AVIATION ADMINISTRATION (Mar. 19, 2015),

public consciousness, there was already movement behind the scenes to integrate drones into the U.S. airspace In 2012, Congress passed the FAA Modernization and Reform Act.[32] Section 332 of the Modernization and Reform Act required the Secretary of Transportation and a number of other stakeholders to "develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system."[33] The FAA's proposed rules deferred privacy concerns to the executive branch.[34] The White House issued a memorandum entitled "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems" on the same day the FAA published its proposed rules.[35] Most of the memorandum focused on the steps agencies must take for privacy protections, accountability, and transparency.[36] The memorandum also established a multi-stakeholder agreement process to "develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private [drone] use in the [National Airspace System]."[37] The multi-stakeholder process was to be initiated by the National Telecommunications and Information

---

http://www.faa.gov/news/updates/?newsId=82225&cid=TW303. Based on these requirements, Amazon must always have a pilot and an observer for every drone. *Id.* This will make it impossible for Amazon to use autonomous drones unless the FAA changes its stance. Atherton, *supra*.

32. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11 [hereinafter FAA Modernization Act].

33. *Id.* § 332.

34. Operation of Small Unmanned Aircraft Systems, *supra* note 14, at 9552.

35. Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, 80 Fed. Reg. 9355 (Feb. 15, 2015) [hereinafter Promoting Economic Competitiveness].

36. *Id.* Privacy protections include examining the existing drone policies and procedures relating to information collected, retained, and used by UAS. *Id.* §(1)(a). Accountability protections include the implementation of policies and procedures to provide training and oversight to agencies wishing to use drones. *Id.* §(1)(c). Finally, transparency protections require agencies to provide notice to the public about where agencies may operate drones, and require agencies to provide summary reports of drone activities from the previous fiscal year. *Id.* at §(1)(d).

37. *Id.*

Administration (NTIA) within 90 days of the publication of the memorandum.[38]

Consistent with the ideas set forth in the presidential memorandum and the FAA Modernization and Reform Act, the FAA and the Department of Transportation agreed to engage in a multi-stakeholder process "to assist in this process regarding privacy, accountability, and transparency issues concerning commercial and private [drone] use in the [National Airspace System]."[39] The multi-stakeholder process led to the National Telecommunications and Information Administration (NTIA), and the Department of Commerce publishing a request for public comment on March 5, 2015.[40] The goal of the process was to "generate a set of non-binding 'best practices' for [drone] operation."[41] The National Telecommunications and Information Administration (NTIA) decided that, given the early stages of the drone industry, non-binding best practices were preferable to a binding code of conduct.[42]

In the request for public comment, the National Telecommunications and Information Administration (NTIA) published a series of preliminary questions concerning privacy.[43] For the purpose of this note, those questions can be grouped into two general categories.

> 1. What "best practices" will mitigate the privacy challenges posed by drones without stifling innovation?[44]
>
> 2. How must a drone be marked to provide the public notice of who is operating the drone? Specifically,

---

38. *Id.*

39. Operation of Small Unmanned Aircraft Systems, *supra* note 14, at 9552.

40. Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems, 80 Fed. Reg. 11,978 (Mar. 5, 2015) [hereinafter Private Use of Unmanned Aircraft Systems].

41. Liz Woolery, *Our Drone Future: Kicking Off the NTIA Multistakeholder Process*, NEW AM: OPEN TECH. INST. (Aug. 6, 2015), https://www.newamerica.org/oti/our-drone-future-kicking-off-the-ntia-multistakeholder-process/.

42. *Id.*

43. *See* Private Use of Unmanned Aircraft Systems, *supra* note 40, at 11,980.

44. *Id.*

> • How can companies and individuals best provide notice to the public regarding where a particular entity or individual operates a [drone] in the [national airspace]?[45]
>
> • What mechanisms can facilitate identification of commercial and private UAS by the public?[46]
>
> • Would standardized physical markings aid in identifying [drones] when the aircraft are mobile or stationary?[47]
>
> • Can [drones] be equipped with electronic identifiers or other technology to facilitate identification of [drones] by the public?[48]

A. The decision to use non-binding best practices has rendered the discussion of those best practices moot in practice.

The public comments on the questions are available on the National Telecommunications and Information Administration's website.[49] In addition to the public comments, the National Telecommunications and Information Administration (NTIA) held six stakeholder meetings that were broadcast around the country.[50] The most recent of these meetings was May 18, 2016.[51] Prior to the November 20, 2015 meeting, several

---

45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Comments on Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft* Systems, NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION (Apr. 24, 2015), https://www.ntia.doc.gov/federal-register-notice/2015/comments-privacy-transparency-and-accountability-regarding-commercial-a.
50. *Multistakeholder Process: Unmanned Aircraft Systems*, NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION (June 21, 2016), http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-unmanned-aircraft-systems.
51. *Id.*

sets of these non-binding best practices have been published. From some of those best practices, the following privacy suggestions arose[52]:

> • [Drone] operators should establish a process, appropriate to the size and complexity of the operator, for receiving privacy, security, or safety concerns. Commercial operators should make this process easily accessible to the public, such as by placing points of contact on a company website. . . . [53]
>
> • Commercial [drone] operators should identify individuals to oversee compliance with applicable laws and drone privacy and security policies. . . . [54]
>
> • Commercial [drone] operators should make a reasonable effort to periodically review compliance with applicable laws and privacy and security policies.[55]

Consistent with the rest of the National Telecommunications and Information Administration (NTIA) discussion, these best practices are also non-binding.[56] Unfortunately, because the "best practices" are non-binding, they have not even been identified.

---

52. *UAS Privacy Best Practices – Discussion Draft v 2*, CENTER FOR DEMOCRACY & TECHNOLOGY (Nov. 19, 2015), http://www.ntia.doc.gov/files/ntia/publications/cdt_uas_best_practices_draft_v2_111615_clean.pdf.

53. *Id.*

54. *Id.*

55. *Id.*

56. Congress attempted to make a drone privacy statute, but the bill died in House committee. Keith Laing, *Lawmakers File Bill to Limit US Drones, Citing Privacy Concerns*, THE HILL (Feb. 14, 2013, 6:14 PM), http://thehill.com/policy/transportation/283195-lawmakers-file-bill-to-limit-domestic-drone-flights. The Preserving American Privacy Act of 2013, H.R. 637, was never enacted. Preserving American Privacy Act, H.R. 637, 113th Cong. (2013). The Preserving American Privacy Act would have applied to drones: "It shall be unlawful to intentionally operate a private unmanned aircraft system to capture, in a manner that is highly offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of a individual engaging in a personal or familial activity under circumstances in which the individual had a reasonable expectation of privacy, through

B. Visual markings are not enough. Drones must be marked with something more identifiable.

According to the FAA's Frequently Asked Questions about drone registration, every drone registrant will be provided with a unique FAA registration number that must be marked on the drone.[57] The number must be affixed in a medium such as, "permanent marker, label, or engraving, as long as the number remains affixed to the aircraft during routine handling and all operating conditions and is readily accessible and legible upon **close visual inspection**."[58] In addition, "[t]he number may also be enclosed in a compartment that is readily accessible, such as a battery compartment."[59]

Return to the story of William Meredith and his sunbathing daughter. Meredith was charged with wanton endangerment and criminal mischief for shooting down a drone.[60] The drone Meredith shot down was worth $1,800 and belonged to David Boggs.[61] Boggs alleges that the drone was almost 200 feet in the air, but Meredith claims it was hovering only ten feet above his home.[62] Consider Meredith's options here under the two essential questions posed. First, what "best practices" should Boggs, as the operator, abide by according to the National Telecommunications and Information Administration's recommendations? And second, how should the drone be marked so that it is easily identified?

Under the Obama administration's circular logic in the "multi-stakeholder process," Boggs, as a drone operator, is supposed to partake

---

the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used." *Id.*

57. *UAS Registration Q&A*, FED. AVIATION ADMIN., http://www.faa.gov/uas/registration/faqs/?cid=TW386 (last modified Sept. 19, 2016).

58. *Id.*

59. *Id.*

60. Ernst, *supra* note 3.

61. *Id.*; Travis Ragsdale, *Interview: Drone Owner Responds to Claims of Privacy Invasion*, WDRB (July 30, 2015, 9:28 PM), http://www.wdrb.com/story/29675427/drone-owner-responds-to-claims-of-privacy-invasion.

62. Ragsdale, *supra* note 61.

in developing the "process" for receiving immediate privacy concerns.[63] Even if the drone was 200 feet above Meredith's property, as Boggs alleges,[64] was Boggs really considering Meredith's privacy? Instead of spying, Boggs states he was merely "having fun with [his] friends and family."[65] But does it matter? To Meredith, the drone was spying on his teenage daughter sunbathing in his own backyard.

Moreover, how was Meredith supposed to identify the drone? The FAA's guidelines suggest that the drone registration markings should be visible "upon close visible inspection," or may even be marked *inside a battery compartment*![66] If the drone were two hundred feet in the air, as Boggs suggests[67], Meredith would have needed binoculars to even have a chance to see the markings. But if the markings were in the battery compartment, there is no way Meredith could see the markings, even if the drone was flying 10 feet high, as Meredith alleged.[68]

Meredith, having no realistic way to identify the drone, shot it down.[69] Boggs called the police, and Meredith was charged with wanton endangerment and criminal mischief.[70] A county court judge, Rebecca Ward, dismissed the charges against Meredith, finding that he was merely defending his right to privacy.[71]

But this begs the question — what, if any, binding precedent do these "best practices" have upon Boggs when he flew his drone over Meredith's property? The answer appears to be none. The FAA avoided

---

63. UAS Privacy Best Practices, *supra* note 52. Because these "best practices" have not been identified, it's unclear what Boggs should have done. Theoretically he could have notified everyone in his flight path about his travel plans; he could have flown more quickly over Meredith's house and not hovered; or he could have simply flown somewhere else.

64. Ragsdale, *supra* note 61.

65. *Id.*

66. *UAS Registration Q&A*, *supra* note 57.

67. Ragsdale, *supra* note 61.

68. *Id.*

69. Ernst, *supra* note 3.

70. *Id.*

71. Justin Peters, *Judge Dismisses Case Against Man Who Shot Down a Drone Over His Property*, SLATE: FUTURE TENSE (Oct. 28, 2015, 5:17 PM), http://www.slate.com/blogs/future_tense/2015/10/28/case_against_william_merideth_for_shooting_down_a_drone_is_dismissed.html.

any responsibility by shoving privacy concerns onto the President.[72] The President created this "multi-stakeholder process" that expressly stated it did not want to create a binding code of conduct for the young drone industry.[73] And now the 'process' that the National Telecommunications and Information Administration (NTIA) recommendations created merely encourages operators themselves to develop a process for receiving privacy concerns!

To summarize, the FAA sought publication of a rule for the commercial use of drones. By seeking publication of a rule, the FAA wanted to create clarity and stability around the increased use of commercial drones. But the FAA did not want to let its rule touch privacy laws, so the President acted. The President did not want to propagate a rule from the top down, so he passed it off to stakeholders. Now those stakeholders are simply suggesting letting the operators, like David Boggs, create the processes for themselves! The passing of the torch has come full circle, and what does the drone industry have to show for it? A set of non-binding practices that individual drone operators may or may not know about, and can choose to follow if they wish.

William Meredith believes he had no other option than to shoot down the drone. "Police told me there was nothing they could do about it. Nobody would do anything about it, so I did something about it."[74] When citizens are resorting to firearms to solve their privacy concerns, clearly something more needs to be done.

III. THE STATES HAVE ATTEMPTED TO ENACT DRONE PRIVACY LEGISLATION, BUT THEIR EFFORTS ARE MERELY A PATCHWORK SOLUTION TO A BROADER PROBLEM.

The states deserve credit because they are at least attempting to enact legislation regulating drones for privacy concerns. "45 states considered 168 [drone] bills" in 2015 alone, and twenty states passed twenty-six

72. Operation of Small Unmanned Aircraft Systems, *supra* note 14, at 9552.
73. Woolery, *supra* note 41.
74. Peters, *supra* note 71.

total bills.[75] In 2016, forty-one states have passed twenty-six total bills.[76] For example, Arkansas amended its voyeurism laws to include drones.[77] California amended its paparazzi laws to encompass drones by preventing paparazzi from trespassing on "the airspace above the land,"[78] and Mississippi added drones to the list of instruments covered under its peeping tom statute.[79] Kansas amended its definition of harassment to include "any course of conduct carried out through the use of an unmanned aerial system over or near any dwelling, occupied vehicle or other place where one may reasonably expect to be safe from uninvited intrusion or surveillance."[80] However, the remaining state drone legislation deals primarily with surveillance, criminal procedure, or hunting activities.[81]

Curiously, popular rapper Kanye West is a voice of reason in the drone privacy debate. In an interview with *Rolling Stone* magazine, West expressed concern over the paparazzi's use of drones to spy on his wife and daughter.[82] "Are there drones flying where she's trying to learn how to swim at age 1? Wouldn't you like to just teach your daughter how to swim without a drone flying? What happens if a drone falls right next to her? Would it electrocute her?"[83] West ultimately decided to sell his Los Angeles home because he could be photographed from the street by the paparazzi.[84]

---

75. *Current Unmanned Aircraft State Law Landscape*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx (last updated Sept. 9, 2016).

76. *Id.* This number is only a reflection of the total legislation up to August 1, 2016. It appears that states are increasing their efforts to enact more drone legislation as drones become more prevalent.

77. ARK. CODE ANN. § 5-16-102 (West 2015).

78. CAL. CIV. CODE § 1708.8 (West 2016).

79. MISS. CODE ANN. § 97-29-61 (West 2015).

80. KAN. STAT. ANN. § 60-31a02(b) (West 2016).

81. NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 75.

82. Kory Grow, *Kanye West Fears Paparazzi Drones, Asked About Nazis in Deposition*, ROLLING STONE (Aug. 7, 2014), http://www.rollingstone.com/music/news/kanye-west-fears-paparazzi-drones-asked-about-nazis-in-deposition-20140807.

83. *Id.*

84. *Id.*

The California legislature responded to the paparazzi complaints when it passed Assembly Bill No. 856.[85] Governor Jerry Brown signed the bill into law on October 6, 2015.[86] Assembly Bill No. 856 amended §1708.8 of the California Civil Code to "expand liability for physical invasion of privacy to additionally include a person knowingly entering into the airspace above the land of another person without permission."[87] Now §1708.8 reads,

> A person is liable for physical invasion of privacy when the person knowingly enters onto the land **or into the airspace above the land of another person** without permission or otherwise commits a trespass in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity and the invasion occurs in a manner that is offensive to a reasonable person.[88]

In essence, the amendment merely applies to the airspace above a person's home or property where drones are most likely to capture images. While this is a positive start, one can imagine a set of scenarios in which this patchwork set of state drone legislation is insufficient to meet new issues of privacy among the states. Two hypotheticals will be discussed to illustrate this point. First, what is the recourse for the Seattle woman whose privacy was invaded by a drone when she was changing in her high-rise apartment?[89] Second, what would happen if I was standing in one state but flying my drone in another? Which state's laws would apply?

---

85. Justin Peters, *Good News for Kanye West: California Bans Paparazzi Use of Drones to Spy on Celeb Homes*, SLATE: FUTURE TENSE (OCT. 9, 2015, 2:50 PM), http://www.slate.com/blogs/future_tense/2015/10/09/california_bans_paparazzi_use_of_drones_to_spy_on_celebrities_at_home.html.

86. CAL. CIV. CODE § 1708.8 (West 2016) *amended by* Assemb. B. 856 (Cal. 2015).

87. *Id.*

88. *Id.* (emphasis added).

89. James Queally, *Seattle Woman Says Drone Seemed to Be Spying on Her*, LA TIMES (June 24, 2014, 5:31 PM), http://www.latimes.com/nation/nationnow/la-na-nn-seattle-peeping-tom-20140624-story.html.

In late June 2014, Lisa Pleiss was undressed in her Seattle apartment building when she noticed a drone flying outside.[90] "It was freaky . . . [y]ou don't expect to be walking around indecent in your apartment and have this thing out there potentially recording you."[91] Pleiss contacted her building concierge, who notified the police.[92] Pleiss was able to take a picture of the drone before it moved out of sight.[93] A Seattle police detective was at a loss on how to enforce the issue.[94] "It's fairly common that technology has outpaced legislation and lawbreaking. At this point, there are no, that we have found yet, laws, at least for Seattle, as to how an unmanned [aerial vehicle] is to be operated in this city."[95]

Assume for a moment that California Civil Code §1708.8 applied here. For drones, §1708.8 specifically applies to "the airspace above the land of another person."[96] The law is great for celebrities like Kanye West who have sprawling estates with ample airspace. But for Lisa Pleiss, in a high-rise building, the drone was not actually *above* her airspace, but merely outside it. And because the Seattle police could not find a specific drone regulation or ordinance applying to the situation, they could only speculate that a law might have been broken.[97]

Other states have adopted remedies that could possibly apply here as well.[98]

- Arkansas prohibits the use of UAS to commit voyeurism.[99] HB 1770 prohibits the use of UAS to collect information about, or

90. *Id.*

91. *Id.*

92. James Queally, *Seattle Woman Says Drone Wasn't Spying on Her after All*, LA TIMES (June 25, 2014, 12:58 PM), http://www.latimes.com/nation/nationnow/la-na-nn-seattle-drone-update-20140625-story.html.

93. *Id.*

94. Queally, *supra* note 89.

95. *Id.*

96. CAL. CIV. CODE § 1708.8 (West 2016).

97. Queally, *supra* note 89.

98. NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 75.

99. H.B. 1349, 90th Gen. Assemb., Reg. Sess. (Ark. 2015); *See also* 2015 Ark. Acts 293.

photographically or electronically record, information about critical infrastructure without consent.[100]

- Florida's search and seizure laws prohibit the use of a drone to capture an image of privately owned property or the owner, tenant, or occupant of such property without consent if a reasonable expectation of privacy exists.[101]

- Mississippi's voyeurism laws specify that using a drone to commit "peeping tom" activities is a felony.[102]

- North Dakota HB 1328 provides limitations for the use of UAS for surveillance.[103]

But these laws are the exception, not the general rule overall for the states.[104] Some local governments or universities are even taking things into their own hands.[105] However, some states are preventing local governments from enacting their own drone laws.[106] Notably, Lisa Pleiss's home state of Washington had made no law concerning drones and privacy, or voyeurism so she had no recourse against those who may

---

100. H.B. 1770, 90th Gen. Assemb., Reg. Sess. (Ark. 2015). *See also* 2015 Ark. Acts 1019.

101. FLA. STAT. ANN. § 934.50 (West 2015).

102. MISS. CODE. ANN. § 97-29-61 (West 2016).

103. H.B. 1328, 64th Gen. Assemb., Reg Sess. (N.D. 2015).

104. NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 75.

105. *U-M announces temporary ban on drones*, DETROIT FREE PRESS, (Feb. 13, 2016, 8:53 AM), http://www.freep.com/story/news/local/michigan/2016/02/13/university-michigan-temporary-ban-drones/80335450/.

106. Maryland SB 370 specifies that only the state can enact laws to prohibit, restrict, or regulate the testing or operation of unmanned aircraft systems. NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 75. This preempts county and municipal authority. *Id. See also* Jenna Portnoy & Josh Hicks, *New Laws in Va., Md. and D.C. Regulate Drones, Uber, Social Media,* THE WASH. POST (June 30, 2015), https://www.washingtonpost.com/local/virginia-politics/new-laws-in-va-md-and-dc-police-drones-uber-and-social-media/2015/06/30/d14f6cc0-1e93-11e5-bf41-c23f5d3face1_story.html. The bill also requires a study on specified benefits. *Id.*

have invaded her privacy.[107] According to Pleiss, "[i]nitially my response was 'that's kind of cool,' and then I very quickly registered there were cameras on it, and then I very quickly realized I was not fit to be on a camera at that point, and that's when the panic set in."[108] Luckily, the drone operator flying outside of Pleiss's building was merely surveying.[109] Pleiss was able to speak with the operator after he had given his name and phone number to Seattle Police and he reassured her that he did not have any pictures of her.[110] The operator intentionally shot at an angle where sunlight would obscure views into the building.[111]

Empirical evidence strongly suggests that not all drone operators are as noble as the one flying outside of Lisa Pleiss's apartment.[112] The system is broken when anyone, sitting in the comfort of his or her own home, backyard, or changing room is not safe from invasions of privacy.[113] State laws have not evolved quickly enough to adapt to the changing realities and possibilities of drones.

---

107. Since that time, Washington has proposed House Bill 1093, which would prohibit voyeurism by drone and require all drones to be labeled with the owner's name and contact information. *Which Bills Are Still Alive at Legislature's Halfway Point*, SEATTLE TIMES (Apr. 25, 2016, 3:11 PM), http://www.seattletimes.com/seattle-news/politics/what-bills-are-still-alive-at-legislatures-halfway-point/.

108. Queally, *supra* note 92.

109. *Id.*

110. *Id.*

111. *Id.*

112. A simple YouTube search reveals numerous instances of drones flying to spy on women on beaches and rooftops. *E.g.*, ViralHog, *Drone helicopter spies topless woman,* YOUTUBE (Oct. 20, 2014), https://www.youtube.com/watch?v=5HOtqFxqmRA; irekim, *Rc DrOnE fLiEs OvEr NuDe BeAcH, and gets chased out*, YOUTUBE (Sept. 3, 2013), https://www.youtube.com/watch?v=PiSEIUnPlEE; THISISZION42303, *Crazed Woman Attacks 17-year old for Flying Drone on Beach*, YOUTUBE (June 18 2014), https://www.youtube.com/watch?v=azFsvay4oLE; Pedro Corpion, *Girl flashes drone on boat*, YOUTUBE (Nov. 7, 2014), https://www.youtube.com/watch?v=LxMpeU1pk7Y; Gonad, *AR Drone 2.0 spying*, YOUTUBE (Mar. 18, 2013), https://www.youtube.com/watch?v=uzjDdVQNFN0; Lane Pearson, *Drone – neighbor spy*, YOUTUBE (Dec. 7, 2014), https://www.youtube.com/watch?v=PqSmaOTiWxM.

113. Even 126 years later, this statement from Warren & Brandeis' influential law review article holds true: "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" Warren & Brandeis, *supra* note 8, at 195.

Another potential issue could arise when drones fly across state lines. Interstate travel or commerce would usually fall under the realm of the federal government,[114] but as I have stated, drone privacy matters have fallen to the states.[115] And when the state drone laws are so varied and disparate,[116] confusion will arise. The question becomes — if I am standing in state A and fly my drone into state B's airspace, which state's laws apply to me?

The United States government has claimed jurisdiction over all airspace in the United States.[117] But that appears to be just for air travel, not air privacy. Legal commentator Renee M. Landers has argued that federal jurisdiction is justified in these situations. "When offenders seek to exploit the jurisdictional limitations of particular states, where an important federal right requires protection, and where state substantive law is otherwise inadequate to achieve full vindication of the rights involved, federal action is justified."[118] Other commentators suggest that the federal government should not have any drone jurisdiction, and that drone privacy laws should be left to individual states.[119]

Overall, many problems exist with the state-by-state privacy model. States are slow to adopt new laws, the new laws are inconsistent with one another, and may even be nonexistent in certain areas.[120] And even if the

---

114. *See* 49 U.S.C. § 40103(a)(1) (2012).

115. *See supra* Section II.

116. *See generally* NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 75.

117. 49 U.S.C. § 40103(a)(1) (2012).

118. Renée M. Landers, *Legislating Federal Crime and its Consequences: Prosecutorial Limits on Overlapping Federal and State Jurisdiction*, 543 THE ANNALS OF THE AM. ACAD. OF POL. AND SOC. SCI. 64, 70 (1996).

119. Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIR. 57 (2013).

120. There is ample evidence from other areas of the law that states have a hard time coming to a consensus regarding laws and regulatory schemes. *See, e.g.*, Susan L. Pollet, *Still a Patchwork Quilt: A Nationwide Survey of State Laws Regarding Stepparent Rights and Obligations*, 48 FAM. CT. REV. 528 (2010) (family laws); Ashley Arthur, *Combating Obesity: Our Country's Need for a National Standard to Replace the Growing Patchwork of Local Menu Labeling Laws*, 7 IND. HEALTH L. REV. 305, 306 (2010) (health labeling laws). In certain instances, the federal government can prod the states with a funding carrot to ensure that all states fall in line. *See, e.g.*, South Dakota v.

state drone privacy laws are enacted, the variation from state-to-state creates a patchwork environment where individual citizens are bound to get hurt.[121]

IV. A MODEL AMERICAN DRONE PRIVACY LAW SHOULD BE BUILT FROM THE FRAMEWORK OF DRONE PRIVACY LAWS FROM THE UNITED KINGDOM AND AUSTRALIA.

The current federal-state dichotomy of drone laws in the United States leaves much to be desired. Other countries are also wading into drone regulation, and ideas from those countries can help the United States answer the two fundamental questions necessary to make drone laws effective: what are the "best practices" for drone operators to use to mitigate privacy concerns without stifling innovation, and how should drones be identified to make those best practices effective?

The law I propose should be viewed as a sweeping statutory law instead of a privacy tort. I propose a statute instead of a tort for two reasons. First, privacy torts have slowly but surely been whittled away by

---

Dole, 483 U.S. 203, 211 (1987) (permitting the federal government to condition the receipt of highway funding on raising the minimum drinking age). Some issues even require actions by the Supreme Court because states are acting too slow or inconsistently. *E.g.*, E. Todd Bennett & James D. Milko, *The Dilemma of Patchwork Solutions: Same-Sex Issues*, 38 MD. B.J. 18 (2005) (providing a history of patchwork state law responses to the Supreme Court's decision in Loving v. Virginia, 388 U.S. 1 (1967)); Obergefell v. Hodges, 135 S. Ct. 2584 (2015) (legalizing gay marriage across the country).

121. An analogy may be drawn between the slow implementation of drone privacy laws and the federal government's slow regulation of ridesharing service Uber. Aaron Sankin, *The Dizzying State of America's Drone Laws*, DAILY DOT (Apr. 24, 2014, 3:28 PM), http://www.dailydot.com/politics/us-state-drone-laws-mess/. There are dozens of examples of violent incidents that have occurred because unregulated Uber drivers have access to passengers and seek to take advantage of them. *See* 'Ridesharing' Incidents, WHO'S DRIVING YOU?, http://www.whosdrivingyou.org/rideshare-incidents (last visited Mar. 16, 2016) (listing dozens of 'ridesharing' incidents). Close to home at Michigan State University, two students reported that a ride share driver made unwanted sexual advances on them, causing the entire campus to be put on alert. Aaron Baskverville, *Michigan State University Students Warned About Ride Sharing Services in Wake of Assaults*, WXYZ DETROIT (Feb. 26, 2016 11:03 PM), http://www.wxyz.com/news/michigan-state-university-students-warned-about-ride-sharing-services-in-wake-of-assaults.

courts.[122] I do not wish for this law to be so limited over time, especially considering that the drone industry is still in its infancy stages.[123] Second, there are already privacy statutes at all levels of government.[124] Although those laws each have their own weaknesses, their mere existence demonstrates the opportunity for this sweeping drone privacy law to be enacted.[125]

A. It does not matter whether the federal government or the states make the law, as long as it is uniform in application and enforcement.

The FAA clearly wants to maintain control of most drone regulations. It has attempted to foreclose the issue in an opinion issued in late 2015.[126] Citing safety concerns, the FAA opinion sought to retain the final say on

---

122. "Dean William Prosser separated privacy cases into four [separate] but related torts—intrusion, appropriation, private facts, and false light." ADAM D. MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 101 (The Pa. State Univ. Press ed., 2010); *see also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 45 (Random House, Inc., 2000). Those four torts were incorporated into the second Restatement of Torts. MOORE, *supra*. However, as Moore mentions, there has been a significant movement away from Prosser's four privacy torts as courts have systematically ruled against them and undermined their efficacy. *Id.* at 116-22.

123. Commentators are calling for the federal government to act quickly and develop a standardized law. *E.g.*, Alan McQuinn, *Don't Let States Make a Mess of Drone Laws*, REPUBLIC 3.0 (Feb. 2015), http://republic3-0.com/dont-let-states-make-mess-drone-laws/. While safety risks are a concern as federal agencies delay publication of clear drone privacy rules, the bigger blow could result when states "inadvertently hamper innovation in an attempt to protect their citizens' safety and privacy." *Id.*

124. MOORE, *supra* note 122, at 101.

125. *Id.* at 111. Moore highlights several federal privacy laws, including the Omnibus Crime Control and Safe Street Act, the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, the Health Insurance Portability and Accountability Act, and the Video Voyeurism Prevention Act of 2004. *Id.* Moore also notes that although the Video Voyeurism Prevention Act contains some very strong privacy protections, its scope is too narrow because it only protects privacy in public. *Id.*

126. Office of the Chief Counsel, *State and Local Regulation of Unmanned Aircraft Systems (UAS) Fact Sheet*, FEDERAL AVIATION ADMINISTRATION (Dec. 17, 2015), https://www.faa.gov/uas/regulations_policies/media/UAS_Fact_Sheet_Final.pdf.

all regulations of the registration and operation of UAS.[127] However, the FAA stated that laws traditionally falling within local and state police power, including voyeurism, should remain in local and state power.[128] Thus, there is room for each state to enact its own drone privacy law, enact the same drone privacy law as all other states, or do nothing.

Foreign countries have recognized the most important "best practice" is to unify privacy laws across member states to achieve uniformity and consistency in the application of those laws. That begins by identifying privacy as a fundamental right.[129] For example, the European Parliament emphasizes that the laws of any nation should not lessen an individual's fundamental right to privacy; rather, national laws should emphasize the right to privacy.[130] In an effort to achieve that goal, the European Parliament has unified laws regarding the processing of personal data and the free movement of such data across country lines.[131] In addition, the Australian advocacy group Liberty Victoria has called for a harmonization of laws between the Australian federal, state, and

---

127. *Id.* at 2. The FAA wants to avoid "fractionalized control of the navigable airspace" and the "patchwork quilt" of state and local regulations that would prevent the FAA from effectively regulating air traffic. *Id.* Essentially, the FAA is claiming field preemption based on Arizona v. U.S., 132 S.Ct. 2492, 2502 (2012).

128. *Id.* at 3. Other examples of local and state police power include the warrant requirement for police to use UAS surveillance, prohibitions on UAS hunting, and prohibitions on attaching weapons to UAS. *Id.*

129. *See, e.g.*, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter Treaty of Lisbon].

130. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 32.

131. *See id* §8. ("Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed").

territorial governments.[132] Therefore, I propose that the true "best practice" for drone operators is a single clear and uniform law that will help with consistency and application across the United States.[133]

B. A unified drone privacy law should set up dual zones of privacy and make drone owners liable for either negligent or reckless behavior.

Liberty Victoria, an advocacy group from Australia, has proposed a civil remedy for privacy violations with surveillance equipment.[134] Specifically, a person is subject to a civil penalty when, without consent, surveillance of private activity occurs and involves:

- "a mental requirement of intent or recklessness;
- an understanding that each person holds a reasonable expectation of privacy with respect to certain activities and locations but not others; and
- appropriate exceptions drawn from current surveillance devices laws to protect beneficial surveillance."[135]

Similarly, the United Kingdom's Data Protection Act of 1998 punishes those who obtain personal data unlawfully.[136] Under this Act, personal data must not be "knowingly or recklessly" obtained or disclosed.[137] In principle, these laws hold merit for a model drone privacy law in the United States. Both the United Kingdom's Data Protection Act

---

132. REECE CLOTHIER ET AL., LIBERTY VICTORIA, THE USE OF DRONES IN AUSTRALIA: AN AGENDA FOR REFORM 6 (2015).

133. As I stated above, I am not advocating for the states or the federal government in particular to pass this law. I believe it would be easiest for the federal government to pass it, but states may have more opportunity given the recent gridlock in Washington. Regardless of how it happens, the law should be implemented across the board.

134. CLOTHIER ET AL., *supra* note 132, at 7.

135. *Id.*

136. Data Protection Act, 1998, c. 29, § 55 (U.K.).

137. *Id.*

and the proposed Australian law recognize each person's reasonable expectation of privacy and allow for surveillance exceptions.[138] Additionally, presence of a mental state requirement in both laws could serve to prevent accidents and needless litigation.[139]

While the Australian and British laws provide a solid framework, they apply broadly to all surveillance. As such, they need to be more narrowly tailored to drone usage to be truly effective. The mental state requirements of intent or recklessness in each law are too protective of drone operators. Liberty Victoria in Australia argues that intent or recklessness will "avoid capturing unintended or innocent surveillance."[140] The group uses an example of someone inadvertently capturing photos of a breastfeeding mother in a maternity ward to make its point,[141] but this example does not necessarily apply to drones. First, drone operators are not going to be flying in a maternity ward. Second, preventing drone operators from seeing breastfeeding mothers, or naked individuals generally in the privacy of their own home, is the goal here.[142] When an individual's privacy has been violated, they should have an adequate remedy. The individual should not have to prove what the operator's intent was when he or she was flying over the home. Instead, the "best practice" should be that operators have a duty of care to not fly over private land. Because operators should have a duty of care, negligence in some form should be the requisite mental state.

---

138. The Data Protection Act does have loopholes for this knowing or reckless standard. *Id.* The statute does not apply when: (a) the information necessary to prevent or detect crime; (b) the person had a reasonable belief that he had a right to collect the information; (c) the person had a reasonable belief that he would have consent; or (d) obtaining or disclosing the information was in the public interest. *Id.* § 55(2)(a)-(d). The proposed Australian law allows for exceptions to protect one's own commercial and economic interests, or to monitor for domestic violence. CLOTHIER ET AL., *supra* note 132, at 15.

139. CLOTHIER ET AL., *supra* note 132, at 7; Data Protection Act, *supra* note 136.

140. CLOTHIER ET AL., *supra* note 132, at 14.

141. *Id.*

142. This law should be confined to areas wherein a person has a "*reasonable expectation of privacy*." *Id.* at 15. According to Liberty Victoria, a reasonable expectation of privacy occurs in "'personal spaces.'" *Id.* "Personal spaces" are where "each person should feel free to express him or herself: in the home, while talking to close friends, while meeting another in a technically public yet secluded space." *Id.*

Modeling the new standardized law after the Australian and British statutes, but substituting negligence, the law would read: [a] person is subject to civil penalty when, without consent, surveillance of private activity occurs and involves:

- "a mental requirement of [negligence];
- an understanding that each person holds a reasonable expectation of privacy with respect to certain activities and locations but not others; and
- appropriate exceptions drawn from current surveillance devices laws to protect beneficial surveillance."[143]

To balance the countervailing interests of drone operators in this new market and citizens seeking to maintain their property rights, a dual zone system should be created. This dual zone system will provide a sphere of protection around citizens by lowering the mental state requirement for invasions of privacy closer to the citizens, and will expand drone capabilities in regions farther from citizens by using a higher mental state requirement. Currently, the FAA will allow drones to fly up to 400 feet high.[144] Thus, there is a region of 400 feet from the ground to the FAA ceiling for drones in which drone operators can fly.[145]

There is also a natural presumption that the closer a drone is to a person, the more invasive that drone becomes.[146] The opposite is also true, as a drone gets farther away, it becomes less intrusive. As such, citizens need more privacy protections when drones are closer, and less

143. *See* Data Protection Act, 1998, c. 29, § 55 (U.K.); *see also* CLOTHIER ET AL., *supra* note 132.

144. Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42063 (Aug. 29, 2016).

145. *Id.* I like to think of this as the FAA ceiling for drones, with the ground as the floor.

146. This concern is especially heightened when one considers the mobility and "inhuman persistence" that drones may use to invade privacy. OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, DRONES IN CANADA: WILL THE PROLIFERATION OF DOMESTIC DRONE USE IN CANADA RAISE NEW CONCERNS FOR PRIVACY? 14 (2013) [hereinafter DRONES IN CANADA].

when drones are farther away.[147] Therefore, I propose splitting a citizen's spheres of privacy into two zones, each having a different mental state requirement for an invasion of privacy claim.[148] The zone closest to the ground will have only a mental state requirement of negligence. This should serve to provide the greatest protection (outside of strict liability) to citizens on the ground while still allowing drone operators to behave responsibly. Higher in the air, the mental state requirement will only be recklessness. Citizens have less of a privacy interest when the drones are higher in the air, and this higher mental state requirement for culpability should sufficiently allow drone operators to use their drones more pervasively.[149] This also complies with the FAA's mandate not to chill the market for drones by preemptively putting too many regulations on them to start.[150]

Enforcement concerns also play a factor in the dual zone model. Later, I propose the use of active radio frequency identification (RFID) as a means to identify drones in encroaching airspace.[151] Current active RFID technology only allows identification at a maximum range of 100

147. There are certain technological limitations with drones, including, "drone operational reliability, image-quality, precision of drone control and of camera control, reliability of image-capture and -transmission, misidentification of surveillance targets, and robustness." Roger Clarke, *The Regulation of Civilian Drones' Impacts on Behavioural Privacy*, 30 COMPUTER L. & SEC. REV. 286, 291 (2014). Currently, there are drones with 4K camera capabilities and flight ranges over a mile long. *The Best Commercial Drones*, BUY THE BEST DRONE (Jan. 15, 2016), https://buythebestdrone.com/best-commercial-drones/. The DJI Inspire 1 drone, for example, can shoot live video in 720p quality. *Id.* As cameras become more and more advanced, the idea is that as drones get closer, our privacy shrinks. It is conceivable to think that someday all drone cameras will see clearly from 400 feet. When (and if) that reality arrives, this may be a moot point.

148. There is an open question as to whether the difference is even relevant. Some researchers wonder whether jurors even notice the difference between recklessness and negligence when punishing actions. *See* Matthew R. Ginther et. al., *The Language of Mens Rea*, 67 VAND. L. REV. 1327, 1329 (2014).

149. *See, e.g.*, Colin Cahoon, *Low Altitude Airspace: A Property Rights No-Man's Land*, 56 J. AIR L. & COM. 157, 159 (1990) (wondering who actually owns the airspace above our homes).

150. Woolery, *supra* note 41.

151. *See* discussion *infra* Section IV(c).

meters, or approximately 300 feet.[152] Splitting the privacy spheres into two zones allows citizens the opportunity to evaluate whether a drone really is invasive and works within existing technology frameworks. Citizens could identify drones in the lower zones simply by using an app on their smartphone. However, the higher zones would require binoculars or some other long-range method. This also serves to protect the privacy rights of drone operators acting reasonably in upper airspace while shielding citizens from nearby drones.

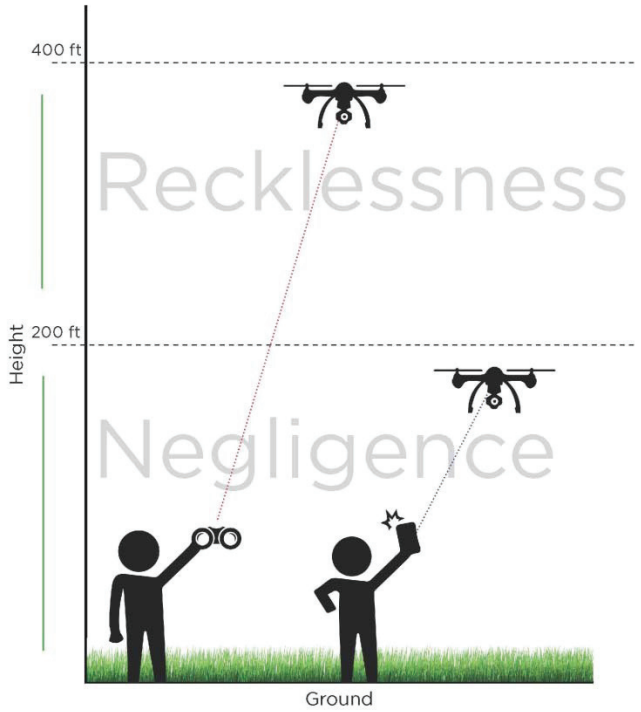
Presumptively, if a citizen can pick up a RFID signal on their phone, the drone will be within 200 feet, and negligence will apply. But if the citizen cannot pick up a RFID signal, the drone is outside of 200 feet, and the recklessness standard will apply. I do note that there is a potential for interference that could skew these ranges,[153] but that should hopefully be mitigated when RFID is applied in open airspace.

The figure below highlights the mental state of each zone[154]:

152. *Active vs. Passive RFID: When Do I Need to Use Active RFID? Or Will Passive RFID Work Just as Well?*, JOVIX, http://atlasrfid.com/jovix-education/auto-id-basics/active-rfid-vs-passive-rfid/ [hereinafter *Active vs. Passive RFID*] (last visited Jan. 18, 2016).

153. *See generally* Dr. Y. Kim and J.G. Yook, *Interference Analysis of UHF RFID Systems*, 4 PROGRESS IN ELECTROMAGNETICS RES. B. 115 (2008).

154. Below 200 feet, a negligence standard will apply. Citizens on the ground can identify drones using their smartphones and the corresponding RFID chips imbedded in the drones. From 200–400 feet, a recklessness standard will apply. Although current RFID technology has limited utility in this range, a citizens can still use binoculars to identify registration markings on the exterior of every drone. No drones are allowed to fly above 400 feet. Diagram courtesy Karinna Sanchez, Michigan State University.



Some could argue that this law is potentially too broad. There is no such thing as absolute privacy; rather, privacy should be viewed on a continuum.[155] Indeed, it also appears that as today's younger generations age, they feel less of a need for privacy protections because their lives are already so digitized.[156] Coupled with society's changing social mores, this makes information that was likely to be kept private a few decades

155. Kevin D. Haggerty, *What's Wrong with Privacy Protections? Provocations from a Fifth Columnist*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 190, 194 (Austin Sarat, ed., 2015).

156. *See* MOORE, *supra* note 122, at 4 ("Many digital natives, those who have grown up with digital technology, have been advocating 'free access' views that would undermine legal protections for privacy.").

ago more palatable today.[157] Another view suggests that the constant presence of drones in the sky could create a "chilling effect" in public spaces and erode privacy.[158] These changing social mores cut against such a sweeping privacy statute applying to drones, especially considering the proliferation of drones that is about to occur.

But privacy has not fallen off the continuum; rather, it should be valued in our society today more than ever. As one commentator notes, "[p]rivacy . . . is a core human value – the right to control access to oneself is an essential part of human well-being or flourishing."[159] And if privacy is truly a social norm, it should be codified into law.[160] The law has adapted to technological advances such as the printing press and radio broadcasting in the past, so there is no reason that it cannot adapt now.[161] Even more so, the immense rise of drones could serve as a privacy catalyst by restoring our idea of a privacy violation.[162]

---

157. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 49 (2000).

158. DRONES IN CANADA, *supra* note 146, at 14 ("[S]ociety's expectations of privacy in public could seriously erode if drone use for surveillance activities . . . could become normalized over time as an accepted interference in our lives.").

159. MOORE, *supra* note 122, at 6.

160. *Id.* at 99. "If legal systems are to reflect important moral norms, then privacy protections must be codified in the law." *Id.*

161. *Id.* at 131. Moore further notes, "In recent times, digital technology and information networking have profoundly changed our notions of public and private. Individual privacy is everywhere threatened. But this need not be so. There have been many technological advances in the past that forced changes in legal systems – the printing press and radio broadcasting are obvious examples. Within the current expansion of digital technology, we need to think more imaginatively about legal protections for privacy." *Id.* at 131-32.

162. DRONES IN CANADA, *supra* note 146, at 14 ("The physical presence and visibility of drones - to the extent that they *are* visible - could actually mean that people would feel observed regardless of how or whether the information was actually used.").

C. All drones should be required to register for an active radio frequency identification tag that will support rapid identification systems.

While it is necessary to develop the unified law applying to all drone operators in the United States, the law is effectively useless if aggrieved citizens cannot identify airborne drones. Currently, drone operators must affix the registration number in a medium such as "permanent marker, label, or engraving, as long as the number remains affixed to the aircraft during routine handling and all operating conditions and is readily accessible and legible upon **close visual inspection**."[163] But given the long-range capabilities of the cameras on new drones, this registration policy appears to disproportionately benefit the drone operators by preventing citizens from identifying drones unless the drones land. Even further, the registration number may be affixed inside the battery compartment.[164] That is equivalent to placing your license plate inside the trunk of your car to avoid detection by the police.[165]

Some commentators have suggested a mixed system of signals, including warning markings, lights, and a drone identification number to be logged in a state registry.[166] But for the reasons stated above, I do not believe that this would be enough. Realistically, citizens on the ground are not going to use binoculars to search out the drone's identification number when the drone is hundreds of feet in the air. Markings and warning lights would also require a degree of training and the dissemination of information to all citizens about their meaning. These solutions all require average citizens to take steps beyond what they already do in their ordinary lives to be free from drone intrusion. An effective drone privacy policy should not make it more difficult for citizens to realize their right to privacy.

Thankfully, a sensible solution potentially exists. Radio frequency identification (RFID) is a generic term for technologies that use radio

163. *UAS Registration Q&A*, *supra* note 57 (emphasis added).

164. *Id.*

165. Thanks for the analogy, Charlie Andrews.

166. A. Michael Froomkin & P. Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 CONN. L. REV. 1, 67 (2015).

waves to automatically identify people or objects.[167] A RFID system consists of a tag, which is made up of a microchip with an antenna and an integrator with an antenna.[168] RFID systems are already used frequently around the country. Toll roads use structures like E-Z Pass system to quickly allow vehicles to pass through toll plazas without stopping.[169] Retailers like Wal-Mart use RFID to monitor customer behavior, while Japanese retailers have used RFID to increase sales efficiency.[170] Perhaps most ubiquitously, credit cards and passports also come with RFID capabilities.[171]

Radio frequency identification comes in two forms: passive and active. Passive tags require power from the RFID reader to power the tag, while active tags use a battery to continuously power the tag and emit a signal.[172] Passive tags only have a short range of approximately three meters, whereas active tags could potentially read up to one hundred meters.[173] Because of their enhanced range and ability to emit their own signal, active tags may cost anywhere between $15 and $100, while passive tags may cost merely $0.15 to $5.00.[174] Passive RFID tags will not be effective when drones are hundreds of feet in the air. Based on this information, I propose that all new drones for civilian use should require an active RFID tag.

The FAA has already considered using RFID registration for drones.[175] Any RFID use would have to be approved by either the Federal Communications Commission or the NTIA.[176] But it is not a

---

167. *Frequently Asked Questions*, RFID JOURNAL, http://www.rfidjournal.com/site/faqs#Anchor-What-363 (last visited Feb. 16, 2016).

168. *Radio Frequency Identification (RFID) Frequently Asked Questions*, AIM, http://www.aimglobal.org/?page=rfid_faq (last visited Feb. 20, 2016).

169. Jennifer E. Smith, *You Can Run, but You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J. L. & TECH. 249, 257 (2007).

170. *Id.* at 257-58.

171. *Id.* at 259-60.

172. *Active vs. Passive RFID*, *supra* note 152.

173. *Id.*

174. *Id.*

175. Nabiha Syed & Michael Berry, *Journo-Drones: A Flight Over the Legal Landscape*, 30 COMM. LAW. 1, 23 (2014).

176. "Within the United States, the Federal Communications Commission (FCC) manages and authorizes all non-federal use of the radio frequency spectrum, including

stretch to imagine the government requiring RFID registration. The government already requires registration for cars, boats, guns, etc. Drone registration would merely be another form of accountability for citizens.

There is also a question of the specific type of information to be provided by the drone registration RFID tag. Namely, when a concerned citizen points their smartphone at a drone, what will he or she see? Two options appear relevant. In one scenario, citizens may see the drone operator's entire name, drone number, address, or any other information as provided by the drone operator when he or she registers the drone with the FAA. In another scenario, only the drone registration number is present. There are certainly privacy concerns for drone operators, and publication of their information for the entire world to see could dissuade some users from complying with mandated drone registration.[177] Further, would a citizen need to know the name of the operator of every drone flying above, or would it only be relevant when the citizen was concerned and wanted to take legal action? In the interest of privacy for the drone operators, I propose that only the drone registration number be made visible via active RFID tags.[178] When a citizen on the ground points their phone at a drone, that citizen should only be able to see the drone's registration number.[179] As noted previously, some commentators have proposed a state registry of drone numbers, similar to the ones

---

state and local government as well as public safety." *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, FEDERAL AVIATION ADMINISTRATION 29 (Nov. 7, 2013), https://www.faa.gov/uas/media/uas_roadmap_2013.pdf [hereinafter *UAS Roadmap*]. "The National Telecommunications and Information Administration (NTIA) manages and authorizes all federal use of the radio frequency spectrum." *Id.* "UAS spectrum operations within the United States need either the approval of the FCC or NTIA and shall not transmit without being properly authorized." *Id.*

177. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000) ("[P]rotecting the acquisition and dissemination of information is an essential means of empowering citizens in a democracy."). Froomkin argues that "informational privacy" is "the ability to control the acquisition or release of information about oneself." *Id.* Further, the most effective way to control information privacy is not to share the information in the first place. *Id.*

178. Each drone is already marked with a registration number, so this will be no different than the current policy. *UAS Registration Q&A*, *supra* note 57.

179. *Id.*

already in use for automobiles.[180] If the citizen wanted to take legal action, a state registry of drone identification numbers (or the FAA registration numbers) can be used to find the identity of the drone operator.[181]

D. Citizens should have a smartphone app that allows them to use radio frequency identification to identify drones flying overhead and notify law enforcement with the push of a button.

In conjunction with a RFID identification tag requirement for all drone registration, the government should concurrently develop a free app for all citizens to download.[182] This hypothetical app would allow citizens to point their cell phone at a flying drone and receive the drone's registration number in return. Using that same app, citizens could transmit the drone registration number and geo-tagged location to police for immediate reporting.[183] By giving citizens the chance to identify drones flying over their property, it will make the sweeping drone privacy law proposed above enforceable. Without a phone app (or another means of reliably identifying drones), any proposed drone law will be toothless.

---

180. Froomkin & Colangelo, *supra* note 166, at 67.

181. Froomkin argues that people have significantly less control when their information is collected into a database. Froomkin, *supra* note 177, at 1464. But even he acknowledges the need for some collection by the government, including situations like applying for a driver's license or getting a job. *Id.*

182. At this point, any drone identification app is purely hypothetical. But 64% of Americans currently own a smartphone, and an app seems like the most convenient way to get identification technology in the hands of all Americans. *U.S. Smartphone Use in 2015*, PEW RESEARCH CENTER (Apr. 1 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

183. The ability to text the police in case of an emergency already exists. *See, e.g.*, *What You Need to Know About Text-to-911*, FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/consumers/guides/what-you-need-know-about-text-911 (last updated Aug. 15, 2016). Further, geo-tagging a location seems like it could be easily achieved. Apps, such as Find My iPhone, already exist that allow the user to see the location of their phone on a map. *Find My iPhone, iPad, and Mac*, APPLE, http://www.apple.com/icloud/find-my-iphone.html (last visited Mar. 16, 2016).

E. The potential drawbacks to using radio frequency identification do not preclude its use.

Two significant obstacles appear with this new licensing system using RFID technology. First, will all drones be within range of the RFID technology? And second, what is the cost of implementing active RFID in all drones, and who will bear the burden of that cost? Each concern is addressed below.

1. Active radio frequency identification does not work up to four hundred feet, but this limitation is used to make the dual zone model feasible.

Current active RFID technology has a range of approximately 100 meters, or 300 feet.[184] The FAA ceiling on drone flight is 400 feet,[185] so clearly active RFID cannot work for the entire flyable drone airspace. However, I believe that issue is solved neatly by bifurcating the zones of privacy. From ground level to 200 feet, active RFID may be used. From 200-400 feet, active RFID will not be used.[186] This makes decisions about which mental state level to enforce very easy, because the citizen will merely be asked how he or she identified the drone.[187] Instead of avoiding RFID technology, as some commentators would,[188] the limitations in the technology should be embraced to create this dual zone system.

---

184. *Active vs. Passive RFID*, *supra* note 152.

185. Gonzalez, *supra* note 23.

186. I recognize that active RFID may be used up to 300 feet, but this is testing the upper bounds of the technology. It will be better to operate within a functional limit that is sure to work rather than to stretch the technology as far as possible when initially implementing it.

187. There is an issue of those citizens that do not use the smartphone app, but want to identify a drone flying under 200 feet. Eyewitness testimony could still apply here.

188. *See* Froomkin & Colangelo, *supra* note 166, at 64.

2. The costs of active radio frequency identification registration and an identification app will be minimized by economies of scale and should be implemented immediately.

The cost of developing a drone identification app is variable. Small apps may generally be developed for less than $10,000, while larger, more complex apps may require up to $150,000 in development costs.[189] There are estimates that long-range RFID readers can cost upwards of $500.[190] Outfitting every drone with a unique RFID tag would also bear a cost. And those RFID tags must be able to transmit their signal at long-range. Those costs would surely add up. But the demand for drones appears to be growing rapidly, and now is the time to introduce these extra costs on drone registration.

While a true estimate of the cost is impossible to provide without access to the technology and app developers, a funding mechanism is abundantly clear. Drone users currently pay $5 to register their drones.[191] This drone registration fee could be increased up to $20 or $25 — especially when some drones sell for more than $1,000 — to pay for the app. While the switch to RFID surely would increase this cost, it seems unlikely that it would reach the upper-bound $100 mark if the government were to require all drones in the registry to use active RFID.[192]

When the drones are registered with active RFID, the drones will emit their own identification signal that may be picked up by an RFID reader

189. *How Much Does It Cost to Develop a Mobile App?,* ASTEGIC (July 10, 2013), https://www.astegic.com/cost-to-develop-a-mobile-app.

190. *See* RFID JOURNAL, *supra* note 167.

191. *FAA Announces Small UAS Registration Rule*, FEDERAL AVIATION ADMINISTRATION (Dec. 14, 2015), http://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856.

192. *See* Abraham Bell & Gideon Parchomovsky, *Of Property and Information*, 116 COLUM. L. REV. 237, 278 (2016) (noting that states providing a single registry service almost always benefit from economies of scale that lower the cost of centralized registries run by a single provider).

held by a citizen on the ground.[193] Which is more effective: citizens using binoculars (which may not be on hand at the time) to identify minute markings on a drone hundreds of feet in the air, or citizens reaching into their pocket, pulling out their smartphone, aiming it at an encroaching drone, and identifying it with a push of a button? Radio frequency identification would serve as a substantial benefit to drone identification. There is a less imposed cost to society if the drone operator bears the burden of advertising the drone's presence or capabilities.[194] And when drones are failing to advertise their presence or capabilities, this will create a reasonable presumption that the drone is dangerous to a person's privacy.[195]

F. The Dual Zone System Would Have Helped William Meredith

Recall the story of William Meredith and his sunbathing daughter. Meredith alleges David Boggs's drone was only ten feet above the ground, while Boggs says the drone was two hundred feet in the air. Under the proposed system, there would be differing results based on the two scenarios. First, if Meredith was correct that the drone was only ten feet in the air, he would have been able to use an app on his smartphone to quickly get the registration number for the drone. After that, he would be required to contact the state registry or the FAA to get Boggs's information. Meredith could then use that information to file a lawsuit where he would be required to show only that Boggs was negligent. Namely, that Boggs did not use reasonable care when flying low over someone's backyard on a summer day because his camera could pick up a minor sunbathing.

In Boggs's scenario, the drone was almost two hundred feet in the air. For the sake of argument, assume that the drone was 210 feet up. In that

193. Active RFID transmits a signal regardless of whether a reader is present in the area, which will make all drones with active RFID tags identifiable at all times. *Active vs. Passive RFID*, *supra* note 152.

194. Froomkin & Colangelo, *supra* note 166, at 60. Froomkin and Colangelo also propose the use of a standardized ex ante warning light system wherein the burden of identifying harmlessness falls upon the drone operator before safe passage for the drone is guaranteed. *Id.* at 62.

195. *Id.* at 60.

case, Meredith would not have been able to identify Boggs's drone using the RFID app on his phone, but would instead have to use binoculars or wait until the drone came lower into his airspace. But because Boggs would have been flying higher, he would only be subject to a recklessness standard and would be more likely to be operating reasonably.

Clearly this system provides an incentive for drone operators to fly higher in the air. The FAA asked drone operators to identify best practices, and this appears to be a best practice — fly higher so that drone cameras do not unwittingly pick up private images that they should not otherwise be seeing. Drone operators can still fly low, as long as they are not negligent. Hypothetically, this would still allow drone operators to fly quickly over land as long as they were not hovering.

While there are many possible scenarios that could play out, RFID and the dual zone system should accomplish a few goals. First, the dual zone system creates incentives for drone operators to operate more freely, at higher airspace, while protecting privacy lower to the ground. Second, RFID allows drones to be identified when the FAA's guidelines would not otherwise require it. Third, the development of a drone identification app makes the dual zone system workable. Without the app (or some other means of rapid identification), any drone privacy law is worthless. Most importantly, now is the time to act on drone identification. Whether the system is RFID, as I propose, or some combination of lights and transponders, the important point is that the system is implemented before a substantial portion of the civilian base uses drones without the identification scheme.[196]

196. *Id.* at 63 (noting "the perfect time to establish a national standard . . . is now, before there is a substantial installed civilian base without standard warning equipment. The more that private owners deploy aerial drones . . . without standard lights, the greater the cost of retrofitting the lights later—or the larger the class of unlighted and grandfathered-in robots, potentially undermining the effectiveness of any warning system.").

VI. CONCLUSION

The current federal guidelines from the Federal Aviation Administration provide a gaping chasm in privacy law enforcement. States have taken some steps to remedy the problem, but inconsistent, slow-to-develop state laws are not effectively solving the problem. The solution is for all states, or the federal government, to pass a sweeping drone privacy law. This drone privacy law, modeled on Australian and British principles and laws, will create two zones of privacy. Close to the ground, drone operators will be liable for negligently conducting surveillance, without an individual's consent, of activities to which an individual has a reasonable expectation of privacy. Higher in the air, recklessness will replace negligence, and drone operators will have more freedom. In conjunction with this sweeping drone law, the FAA should concurrently and immediately mandate all registered drones be tagged with a long-range radio frequency identification mechanism. This step is necessary to allow individuals with a reasonable expectation of privacy to identify drones flying overhead. Without the identification step, the law is a paper tiger, and the citizens of the United States will experience a greatly diminished sphere of privacy.