Richmond Journal of Law and Technology

Volume 21 | Issue 4 Article 4

2015

Commercial Drones and Privacy: Can We Trust States with 'Drone Federalism'?

Robert H. Gruber

COMMERCIAL DRONES AND PRIVACY: CAN WE TRUST STATES WITH "DRONE FEDERALISM"?

Robert H. Gruber*

Cite as: Robert Gruber, *Commercial Drones and Privacy: Can We Trust States with "Drone Federalism"?*, 21 RICH. J.L. & TECH. 14 (2015), http://jolt.richmond.edu/v21i4/article14.pdf.

I. INTRODUCTION

[1] Judge Andrew Napolitano said recently of unmanned aircraft systems ("UAS"), or "drones,"[1] that "[t]he first American patriot that shoots down one of these drones that comes too close to his children in his backyard will be an American hero."[2]

* Author Robert H. Gruber is a litigation associate at Greenberg Traurig, LLP. This article is presented for informational purposes only, and it is not intended to be construed or used as general legal advice nor as a solicitation of any type. The author gratefully acknowledges the assistance of Jordan Grotzinger, Adam Siegler, John Villasenor, and Ivan Perkins.

[1] Drones are also commonly referred to as "UAVs" or "Unmanned Aerial Vehicles." *See* Matt McFarland, *Here's What Drone Advocates Love and Hate About the FAA's Proposed Rules*, WASH. POST (Feb. 15, 2015, 6:57 PM), http://www.washingtonpost.com/blogs/innovations/wp/2015/02/15/heres-what-drone-advocates-love-and-hate-about-the-faas-proposed-rules/, *archived at* http://perma.cc/L2TD-JTTD (using "drone" "UAV" and "UAS" as interchangeable terms). This article uses "drone," "UAV," and "UAS" more or less interchangeably, but with "UAS" referring to the entire system (including the operator), and "UAV" referring to the aircraft alone.

[2] Steve Watson, *Judge Napolitano: First Patriot to Shoot Down a Government Spy Drone Will Be a Hero*, INFOWARS.COM (May 16, 2012), http://www.infowars.com/judge-napolitano-first-patriot-to-shoot-down-a-government-spy-drone-will-be-a-hero/, *archived at* http://perma.cc/RTP7-4MMM.

[2] If you sympathize with that sentiment, you are not alone. Much of the discourse on domestic drone use has been informed by concerns over privacy implications.[3] The judge's statement epitomizes a kind of visceral reaction—one that many share—to the idea of unmanned aircraft monitoring our every activity. In the broadest sense, this article invites readers to question that reaction. Why would one fly a drone into an ordinary citizen's backyard? Wouldn't safety regulations (and existing privacy laws) prohibit that behavior? Should we really be shooting these things out of the sky?

[3] Congress has instructed the Federal Aviation Administration ("FAA") to present a plan for integrating UAS into American airspace by September 2015.[4] Right now, UAS are authorized for only a handful of uses, primarily public entities.[5] Commercial UAS are prohibited,[6] with few exceptions[7]—although this is likely to change when the FAA's most recent proposed rules go into effect.[8]

---

[3] *See, e.g.*, Chris Schlag, *The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights*, 13 PITTSBURGH J. TECH. L. & POL'Y 1, 22 (2013) (arguing that "proactive steps should be taken by both the Legislature and the Judiciary to ensure individual privacy rights are not eroded with the incorporation of [UAV] technology into our daily lives.").

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

[5] *See* John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL'Y 457, 471–73 (2013).

[6] *Id.* at 471.

[7] *See, e.g.*, Nick Lavars, *U.S. Gives Hollywood Film Studios Green Light on Drone Use*, GIZMAG (Sept. 26, 2014), http://www.gizmag.com/us-hollywood-exemption-film-drone-use/33994/, *archived at* http://perma.cc/GEH3-TAVN.

[8] Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems ("NPRM"), 80 Fed. Reg. 9544,9590 (Feb. 23, 2015).

[4] At this stage, it is impossible to accurately predict the scope of the future UAS industry. Its potential benefits are vast and varied: beyond mere job creation, drones will contribute to efficiency in various industries and aspects of society. This is particularly true in the commercial sphere, where competition and innovation can drive progress towards functions far removed from the individual surveillance people fear. UAS have already proven useful in functions from crop monitoring[9] to gathering atmospheric data.[10] Domino's Pizza made headlines when it announced the development of delivery UAS systems, as have other companies—and while some skeptics dismissed the press releases as "publicity stunts,"[11] it is not too difficult to imagine a future in which packages appear on our doorstep out of the sky.[12] Recently, Facebook announced a plan that epitomizes the benevolent possibilities of commercial UAS.[13] It has

[9] *See* Chris Anderson, *Agricultural Drones, Relatively Cheap Drones with Advanced Sensors and Imaging Capabilities are Giving Farmers New Ways to Increase Yields and Reduce Crop Damage*, 17 MIT TECH. REV. 3, 58, 60, (2014) *available at* www.technologyreview.com/featuredstory/526491/agricultural-drones/, *archived at* http://perma.cc/RA6G-FR8J.

[10] *See* Tereza Pultarova, *Atmospheric Research Drones Developed by U.K. scientists*, E&T (Aug. 2, 2013), http://eandt.theiet.org/news/2013/aug/atmoshperic-drones.cfm, *archived at* http://perma.cc/AMW3-LTYX.

[11] *See, e.g.*, David Hambling, *Drone Deliveries: Beyond the Publicity Stunt*, WIRED (Apr. 6, 2014), http://www.wired.co.uk/news/archive/2014-04/06/drone-deliveries, *archived at* http://perma.cc/8ZZY-2WSW.

[12] *See* Jenny Stanton, *Drone Delivery Is Here! China's Largest Mail Firm to Deliver More Than 1,000 Packages A DAY to Remote Areas Using Fleet of Aircraft*, DAILY MAIL (Mar. 24, 2015, 11:28 AM), www.dailymail.co.uk/news/peoplesdaily/article-3009593/Drone-delivery-China-s-largest-mail-firm-deliver-1-000-packages-DAY-remote-areas-using-fleet-aircraft.html, *archived at* http://perma.cc/4GU9-7PBZ.

[13] *See* Josh Constine, *Facebook Will Deliver Internet Via Drones with "Connectivity Lab" Project Powered by Acqhires from Ascenta*, TECH CRUNCH (Mar. 27, 2014), http://techcrunch.com/2014/03/27/facebook-drones/, *archived at* http://perma.cc/7N7S-GEFJ; Victor Luckerson, *Facebook Reportedly Wants to Buy a Drone Company*, TIME (Mar. 4, 2014), *available at* http://time.com/12395/facebook-drones-titan-aerospace/,

purchased the U.K.-based company Ascenta, which manufactures solar-powered aircraft that can stay aloft at high altitudes for years at a time. Facebook's goal? Providing Internet access in areas where traditional connections are impractical or impossible.[14] Even though commercial UAS flight is still largely prohibited in the United States, the battle over drone regulation has already begun, fixated largely on imagined harms to people's privacy.[15] And the privacy advocates are winning: more than twenty states have passed laws restricting UAS operations.[16] Many of these address law enforcement surveillance, but an increasing number of states are proposing—and enacting—restrictions on private and commercial aircraft. For example, a bill proposed and enrolled in Texas makes it a misdemeanor to collect an image of a person's land without consent.[17] Other states are considering similar legislation.[18] One town in

archived at http://perma.cc/HW6D-XSTM.

[14] *See* Luckerson, *supra* note 13. In acquiring Ascenta, Facebook passed on Titan Aerospace, a similar startup that was later snapped up by Google for the same purpose: remote Internet service delivery.

[15] *See* Villasenor, *supra* note 5, at 459–60, 487; *see also* Margot E. Kaminski, *The Rules of the Sky*, SLATE (Feb. 25, 2015, 7:47 AM), http://www.slate.com/articles/technology/future_tense/2015/02/faa_small_commercial_drone_rules_don_t_adequately_address_privacy_concerns.single.html, *archived at* http://perma.cc/3WMJ-SJZU (addressing the federal privacy issues and First Amendment concerns regarding state privacy regulations likely to arise in light of the FAA's "less [than] stringent" proposed rules regulating small commercial drones).

[16] *See* Rich Williams, *Current Unmanned Aircraft State Law Landscape*, NAT'L CONF. OF STATE LEGISLATURES (Dec. 29, 2014), *available at* http://www.ncsl.org/research/civil-and-criminal-justice/current-uas-state-law-landscape.aspx, *archived at* http://perma.cc/XQH5-8W6P.

[17] *See* Texas Privacy Act, H.B. No. 912, 83d Leg. (Tex. 2013).

[18] *See* Allie Bohm, *Status of 2014 Domestic Drone Legislation in the States*, ACLU (Apr. 22, 2014, 10:32 AM), *available at* https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states, *archived at* https://perma.cc/5ENY-V8C5?type=source [hereinafter *Status of 2014 Domestic Drone Legislation*] (providing a

Colorado must have gotten Napolitano's memo—it considered issuing "drone hunting licenses" that would authorize its citizens to shoot any unpiloted aircraft.[19]

[5] This sort of legislation is both premature and problematic, particularly with respect to the kind of drones that will be used for commercial or civil purposes (as opposed to law enforcement purposes). It is premature because legislators cannot foresee—and therefore cannot balance—all of the potential benefits and harms of commercial drone use. Many of the privacy interests purportedly advanced by restrictive legislation are already protected by other areas of the law.[20] It is problematic because inconsistent and overly-restrictive regulations (1) potentially violate the First Amendment right to gather information and (2) threaten to chill industry growth.[21] The harms such legislation causes are analogous, in a sense, to those that would have arisen if states had created a patchwork of Internet privacy laws several years before the development of the World Wide Web.[22] Right now, the United States leads the pack in

status chart with each state proposal).

[19] *See* Nidhi Subbaraman, *Open Season on Drones? Town Split over Licenses to Hunt Unmanned Aircraft*, NBC NEWS (Aug. 8, 2013, 3:36 PM), http://www.21alive.com/nbc33/news/Open-Season-On-Drones-Licenses-To-Hunt-Unmanned-Aircraft-In-Colorado-218987751.html, *archived at* http://perma.cc/U6RP-5VYZ.

[20] *See, e.g.*, Villasenor, *supra* note 5, at 498–508.

[21] *See* Timothy M. Ravich, *The Integration of Unmanned Aerial Vehicles into the National Airspace*, 85 N.D. L. REV. 597, 621 (2009) ("For the UAV industry to thrive, insurers, engineers, manufacturers, operators, military tacticians, and other stakeholders must have a firm and predictable set of laws that establish rights and liabilities emanating from UAV operations.").

[22] *See* Villasenor, *supra* note 5, at 517 ("If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in

UAS technology. If the current legislative pattern continues, the U.S. might very well drive a market with incredible potential overseas, to more open-minded nations.[23]

[6] Is restrictive legislation nevertheless justified, as a means of vindicating legitimate privacy interests?[24] Perhaps not, particularly where commercial UAS use is concerned. There are few cognizable circumstances in which using drones to monitor individual people will be profitable for non-government actors and entities.[25] First, a primary advantage of unmanned aircraft is that they can go swiftly and easily where people *cannot*. UAS could be used profitably to survey mines, monitor power lines in remote areas, collect traffic-flow information,

ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.").

[23] *See, e.g.*, Zenon Evans, *Will the Government Test Drones in* Your *State?*, REASON.COM (Dec. 31, 2013, 2:19 PM), http://reason.com/blog/2013/12/31/will-the-government-test-drones-in-your, *archived at* http://perma.cc/N85J-Z7VY ("Brendan Schulman, who works as special counsel for the drone industry, [said] 'what we've experienced the past several years is a lot of regulatory delay. In the meantime, other countries have moved ahead with permitting and embracing commercial use. Countries like Australia, Canada and the United Kingdom already have a framework for commercial use of drones. That's where you'll see companies going to do the work. That's where you see investment dollars going.'").

[24] *See generally* Schlag, *supra* note 3, at 22 (arguing that "proactive steps should be taken by both the Legislature and the Judiciary to ensure individual privacy rights are not eroded with the incorporation of [UAS] technology into our daily lives.").

[25] Admittedly, drones could potentially be used to target celebrities. But there are ways to prevent celebrities' privacy from being invaded—California's Anti-Paparazzi law is one such example—that do not also restrict drone operations. To outlaw drone flights in the pursuit of protecting celebrities' privacy would be a bit like outlawing smartphones to prevent people from hacking photographs.

spray and monitor crops, and so forth. Some predict that eighty-percent of commercial drones will be used for agricultural purposes[26]—so the majority will seldom even accidentally interfere with individual privacy interests. As one person put it, "corn doesn't mind if you watch it."[27] Second, even if a particular commercial drone's images could be processed and linked to individuals' identities, what would justify the cost of such directed monitoring? Demographic information may be valuable, but our phones and Internet activity paint a cheaper and more accurate picture of consumer activities—where individuals go, where they shop, and what they buy.

[7] The global market for UAS is growing fast.[28] At the moment, the best available UAS technology belongs to the United States and Israel.[29] Developed for military purposes, this technology nevertheless has massive export potential for civil and commercial uses.

---

[26] *See* Christopher Doering, *Growing Use of Drones Holds Promise of AG Transformation*, ARGUS LEADER (Mar. 30, 2014, 12:25 AM), http://www.argusleader.com/story/news/2014/03/29/growing-use-drones-poised-transform-agriculture/7073585/, *archived at* http://perma.cc/TW2Y-G6MX.

[27] D.C. Denison, *Maker Pro Newsletter - 10/17/13*, MAKE: (Oct. 18, 2013, 4:45 PM), http://makezine.com/2013/10/18/maker-pro-newsletter-10-17-13/, *archived at* http://perma.cc/FND7-EW48.

[28] *See* Benjamin Kapnik, *Unmanned But Accelerating: Navigating the Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System*, 77 J. AIR L. & COM. 439, 440–41 (2012) ("Annual worldwide unmanned aircraft expenditures are expected to grow from $6.6 billion to $11.4 billion within a decade. Although the market for civil use currently comprises less than 2% of the worldwide market for unmanned aircraft, that could change over the next several years as technology advances and as legislation and regulations allow broader use of unmanned aircraft in the NAS.").

[29] *See* Tia Goldenberg, *Israel Leads Global Drone Exports as Demand Grows*, YAHOO NEWS (June 5, 2013, 3:44 PM), http://news.yahoo.com/israel-leads-global-drone-exports-demand-grows-194424173.html, *archived at* https://perma.cc/SN8N-435M?type=source.

[8] However, the United States' monopoly on UAS technology may already be eroding. In 2013 Israel surpassed the U.S. as the chief exporter of UAS technology—although Israel remains second to the U.S. in production.[30] What accounts for this discrepancy? A regulatory barrier: the companies that develop our military drones are restricted from marketing their technology elsewhere.[31] China and other countries are now entering the ring.[32] By competing in the global market, the U.S. can realize all the benefits of a multi-billion dollar industry once the FAA opens up the national airspace[33]—which it is poised to begin doing soon—but only if the U.S. avoids establishing a draconian regulatory framework for commercial UAS.

[9] This Article focuses on commercial UAS, and on the legal frameworks—both current and potentially forthcoming—surrounding

[30] *Id.*

[31] *See U.S. Drone Exporters Losing Out to Israeli, Chinese Competitors*, HAMODIA, Feb. 14, 2014, at 6, *available at* http://hamodia.com/2014/02/13/u-s-drone-exporters-losing-israeli-chinese-competitors/, *archived at* http://perma.cc/94LW-5Z3A [hereinafter *U.S. Drone Exporters*] ("Exports of drones are tightly controlled by an agreement signed by members of a group called the Missile Technology Control Regime, which includes the United States, Britain, Canada, France, Germany, Italy, and Japan. The group has since expanded to 34 countries but Israel and China aren't members. . . . The controls give rival drone makers from countries such as Israel and China a chance to win more business in the growing global market for unmanned aerial vehicles, which one group projects to more than double in the next decade. U.S. arms makers have been lobbying the government for several years to loosen the restrictions so they can sell their systems to more countries.").

[32] *U.S. Drone Exporters*, *supra* note 31.

[33] Bill Wood, *Wood on Plastics: Aerospace Market Losing Altitude*, PLASTICS TECHNOLOGY (July 2010), http://www.ptonline.com/columns/wood-on-plastics-aerospace-market-losing-altitude, *archived at* http://perma.cc/L2MB-DR3D. ("The U.S. currently holds a tremendous edge in UAV technology and production, but Europe and Asia are trying to catch up. Many analysts believe that the commercial potential for UAV's is nearly unlimited. The only glitch is getting access to civilian airspace.").

them.[34] Part I provides a brief background of the politically-charged context within which UAS regulation is being developed. Part II examines two critical issues in the UAS regulatory debate: (1) the extent to which the "third-party doctrine" will apply to information captured by commercial UAS; and (2) the boundaries of First Amendment protection of "information gathering." Part II also outlines existing state and federal laws governing civil drone use. Part III examines approaches the United States could take in regulating commercial drone use. Ultimately, the article concludes that the federalism model will stifle the market for UAS aircraft and technology, unless Congress acts to create a baseline federal scheme that assuages privacy concerns without hindering industry growth.

II. BACKGROUND

[10] There is nothing novel about unmanned flight as a general concept. As John Villasenor has put it, "model airplane hobbyists have known for decades that an airplane can be flown without a human in the cockpit."[35] Nor is there anything new using aircraft, model or otherwise, to take pictures: if someone visited a hobby store during the 1990's, they might have seen toy rockets outfitted with cameras. Light the fuse, watch the rocket fire upwards, and once it drifted down (with the aid of a parachute), one would be rewarded with a chip full of aerial views of the neighborhood.

[11] The drones heard of today are simply an extension of this concept, the natural result of improvements in communications and imaging technology.[36] Even weaponized drones are not themselves a recent idea.

[34] This Article uses "commercial," "civil," and "private" interchangeably to refer to what the FAA has designated as "civil" aircraft—essentially, any aircraft not operated by a public entity.

[35] Villasenor, *supra* note 5, at 458. He's right—I've been flying model airplanes for twenty years myself.

[36] *Id.* at 464. ("One key factor contributing to [UAV growth] is the continuing advance of

Unmanned aircraft were deployed in the Vietnam War; unsuccessful attempts date even farther back.[37] Israel developed UAVs with real-time surveillance capabilities in the 1970s and 80s.[38]

[12] However, UAS's military proliferation after the terrorist attacks on September 11, 2001 (and the ongoing firestorm of media coverage that resulted) cast the idea of "drones" in a decidedly negative light.[39] As a result, the discussion over integrating UAS into domestic airspace has been dominated by skepticism. Add in recent revelations about the extent of NSA surveillance and data collection—which grant legitimacy to growing concerns about the state of our privacy protections—and it is a very bad time to be a domestic drone.[40]

[13] This is particularly unfortunate because the vast majority of domestic UAS applications, whether civil or private, are beneficial.

computing, imaging, and communications technologies.").

[37] *Id.* at 464.

[38] *Id.*

[39] Even my own experiences demonstrated a change in attitude. As a teenager I often traveled to compete in model airplane competitions, and it was eerie to watch people's—particularly TSA agents'—attitudes towards my models change from interest to skepticism. Toys became "drones," and by the end of my career it took a letter from the head pilot of United Airlines to get my model airplane overseas in one piece.

[40] *See, e.g.*, Wendie Kellington, *Unmanned Air Systems and Regulating Navigable Airspace*, ALI ALBA LAND USE INST. 1 (Aug. 14–16 2013), *available at* http://www.wkellington.com/pdf/2013/Unmanned-Aerial-Systems-and-Regulating-Navigable-Airspace.pdf, *archived at* http://perma.cc/G8FD-RLEY ("The military's use of UAVs in the hunt for al Qaeda operatives created an indelible public image of mindless beasts carrying out a distant programmers' messy bidding. Moreover, reports of UAVs being developed for purposes like hiding from and sneaking up on people have not generated an enthusiastic reception for domestic use of the technology. Civil demand for domestic UAVs thus finds itself colliding with a culture of wariness, creating difficult barriers to domestic UAV use and slowing regulatory response.").

Indeed, if these aircraft are as successful at home as they have (arguably) been in their military applications, the market for new and varied models has incredible potential. Unmanned flight can contribute to efficiency, productivity, and safety in a potentially unlimited number of areas.[41] Farmers can use them to crop-dust safely.[42] Civil engineers can monitor traffic and power lines. An enterprising farmer in Ireland, apparently, has discovered that drones are wonderful at herding sheep.[43] In the coming decades, individuals may even receive pizzas and Internet service via drone.[44]

[14] Nevertheless, integrating UAS into U.S. airspace raises a number of concerns. The foremost of these relate to privacy and safety. What follows is an overview of the frameworks that will govern the regulation of UAS, as well as an overview of existing regulations themselves.

III. SOURCES OF REGULATION

A. Fourth Amendment: the Third-Party Doctrine

1. Precedent

[15] The Fourth Amendment restricts government (not private actors),

[41] *Id.* ("According to the Government Accountability Office (GAO), current domestic use of UAVs includes law enforcement, monitoring or fighting forest fires, border security, weather research and scientific data collection by the federal government.")

[42] As of the writing of this article, Japan has successfully implemented UAVs towards this purpose.

[43] *See* Michael Franco, *Watch This Drone Shepherd Round Up Its Flock on an Irish Farm*, CNET (Mar. 30, 2015, 11:52 AM), http://www.cnet.com/news/watch-this-drone-shepherd-round-up-a-flock-on-a-farm-in-ireland/, *archived at* http://perma.cc/7YUF-4RRU.

[44] *See* Hambling, *supra* note 11.

so some might question its place in an article about commercial drones. For this reason, and because others have discussed the subject in detail,[45] what follows is a primer on a particular piece of Fourth Amendment law—the "third-party" or "*Miller*" doctrine. The manner in which this doctrine is applied to data collected by UAS will bear significantly on developing policies regarding commercial drone use. Articulated in *United States v. Miller*, this doctrine permits the government to obtain information from third parties, in certain circumstances, without the procedural hurdles that would otherwise present themselves if the information were sought directly from a suspect.[46]

[16] In *Miller*, the trial court convicted the defendant of various federal offenses involving his operation of an unlicensed whiskey still.[47] On appeal, he argued that the trial court committed error in failing to suppress records obtained from his two banks.[48] The Court of Appeals for the Fifth Circuit reversed the conviction "on the ground that a depositor's Fourth Amendment rights are violated when bank records . . . are obtained by means of a defective subpoena."[49] The Supreme Court granted certiorari, and reversed again.[50]

[17] In doing so, the Court rejected the argument that the defendant retained an expectation of privacy in information relayed to the bank.[51]

[45] *See generally* Villasenor, *supra* note 5 (discussing government operation of unmanned aircraft and the Fourth Amendment).

[46] *See* U.S. v. Miller, 425 U.S. 435, 444 (1976).

[47] *See id.* at 437.

[48] *See id.* at 436.

[49] *Id.* at 437.

[50] *Id.* at 435.

[51] *Miller*, 425 U.S. at 442.

Even though the bank was required by statute to maintain its records, and the defendant was required to release the information in order to do business with the bank, the Court cited prior holdings in concluding:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[52]

[18] The third-party doctrine has since formed the basis for a variety of notable Supreme Court opinions. In *Smith v. Maryland*, police—without a warrant or court order—asked a telephone service provider to install a "pen register" in its offices in order to track a suspect's phone calls.[53] The Court held, in a decision that has wielded significant influence since the development of the Internet,[54] that the defendant had "assumed the risk that the company would reveal to police the numbers he dialed."[55] The court noted that the register recorded only the numbers dialed—not the content of the conversations, which presumably would have been entitled to greater protection.[56]

---

[52] *Miller*, 425 U.S. at 443.

[53] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[54] *See* John P. Collins, Project, *The Third Party Doctrine in the Digital Age*, N.Y.L. SCH. JUST. ACTION CTR. 6 (2012), *available at* http://www.nyls.edu/documents/justice-action-center/student_capstone_journal/cap12collins.pdf, *archived at* http://perma.cc/CXA7-HLFN ("The significance of this decision was not readily apparent, but by expanding the third party doctrine to include information revealed to a machine carrying out a routine task, the court laid a foundation that would drastically expand the reach of the third party doctrine upon the advent of the [I]nternet.").

[55] *Smith*, 442 U.S. at 744.

[56] *Id.* at 741, 744.

[19] Later, in *California v. Greenwood*, the Court extended its *Smith* analysis to rule that the contents of a suspect's garbage received no Fourth Amendment protection.[57] The Court reiterated its observation that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[58] Therefore, the Court held, procuring the suspect's trash from his garbage collector worked no Constitutional harm.[59] The Court also stressed, however, that the suspect's transmission of information *to the public in general* deprived him of a Fourth Amendment claim: "Hence, 'what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'"[60] The garbage bags in question were accessible not only to the trash collector, but to "animals, children, scavengers, snoops, and other members of the public."[61]

[20] The final Supreme Court case that deserves mention is *United States v. Jones.*[62] In *Jones*, the government procured a warrant to place a GPS device on a suspect's vehicle; the warrant provided that the device should be secured within ten days in the District of Columbia.[63] Instead, the device was attached to the suspect's vehicle in Maryland and on the

[57] California v. Greenwood, 486 U.S. 35, 40 (1988).

[58] *Id.* at 41.

[59] *Id.* at 40 ("respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so.").

[60] *Id.* at 41 (citing Katz v. United States, 389 U.S. 347 (1967)).

[61] *Id.* at 40.

[62] United States v. Jones, 132 S. Ct. 945 (2012).

[63] *Id.* at 948.

eleventh day, voiding the warrant.[64] The government monitored the vehicle's position for twenty-eight days, and at one point changed the battery in the device—also in Maryland.[65] The Court unanimously held that the month-long monitoring of the vehicle's position, without a proper warrant, violated the Fourth Amendment.[66]

[21] In *Jones*, the Court neither relied on nor repudiated the "third-party" doctrine.[67] The case nevertheless merits note because of the varied perspectives articulated in not only the Court's opinion, but also in certain Justices' concurrences.[68] Scalia wrote for the majority.[69] His opinion highlighted the trespass that had occurred when law enforcement placed the GPS device on the suspect's automobile.[70] It noted a turn in Fourth Amendment jurisprudence that had occurred in the latter half of the twentieth century, beginning with *Katz* (the source of a test that has dominated more recent Fourth Amendment jurisprudence: the "reasonable expectation of privacy" test).[71] Before that, the Court stated, Fourth Amendment rights had turned on the more traditional law of trespass.[72]

[22] In an originalist interpretation typical of Scalia's Constitutional

[64] *Id.*

[65] *Id.*

[66] *Id.* at 954–57.

[67] *See Jones*, 132 S. Ct. at 952.

[68] *See id.* at 948–64.

[69] *Id.* at 948.

[70] *Id.* at 949.

[71] *Id.* at 949–50.

[72] *Jones*, 132 S. Ct. at 949–50.

readings, the Court held that *Katz's* "reasonable-expectation-of-privacy" test was not exclusive; rather, it complemented this more traditional, trespassed-based line of Fourth Amendment law.[73] The Court's decision rested on the fact that the government had "physically occupied private property for the purpose of obtaining information."[74] Such an intrusion, the Court reasoned, would "no doubt . . . have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[75] The Court rejected the government's principle argument (tied to *Katz* and its progeny): that Jones held no reasonable expectation of privacy in (1) the undercarriage of his car or (2) his movements on public roads.[76] It distinguished prior cases involving mere observation, with no accompanying trespass. Despite its reliance on the government's trespass as the basis for its holding—and its distinguishing of similar cases without that element—the majority did not address whether the extended monitoring achieved here would have violated the Fourth Amendment if no trespass had occurred. In fact, it explicitly avoided that question: "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[77]

[23] *Jones* also generated two concurring opinions. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, would have held that Jones's Fourth Amendment rights to privacy were violated based solely on *Katz's* "reasonable expectation of privacy" test.[78] They concluded four

[73] *Id.* at 952.

[74] *Id.* at 949.

[75] *Id.*

[76] *Id.* at 950–52.

[77] *Jones*, 132 S. Ct. at 954.

[78] *Id.* at 957–64.

weeks of location monitoring contradicted reasonable expectations:

> The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated. Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.[79]

[24] Justice Sotomayor joined the majority in agreeing that a trespass-based approach functions as a baseline of constitutional protection, but she wrote separately to address her own concerns with electronic monitoring.[80] She agreed with Alito's concurrence insofar as, under the *Katz* analysis, the government's long-term monitoring of Jones violated his expectation of privacy.[81] She went further in suggesting that even certain types of short-term electronic monitoring might violate the Fourth Amendment.[82] Finally, she questioned the continuing validity of the third-party doctrine in the digital age:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves

[79] *Id.* at 963–64 (internal citations omitted).

[80] *Id.* at 954–57.

[81] *Id.* at 955–56.

[82] *Jones*, 132 S. Ct. at 955–56.

> to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[83]

2. Application of Third-party Doctrine to Information Captured by Commercial Drones

[25] What can the foregoing cases teach us about information captured by commercial drones? First, these aircraft—and the data they capture—will not fall neatly into any particular line of Supreme Court precedent. *Miller's* original formula highlighted the "voluntary" nature of the defendant's disclosures to the bank, which were made for the purpose of receiving services.[84] This relationship is not likely to exist in cases where commercial UAS capture images of private citizens. Perhaps a "Facebook drone" that provides Internet may keep records of Internet activity, but any images it captures would be unrelated to the service provided.[85] Relatedly, in *Smith*, the Court was concerned not just with voluntary disclosure to a third party, but also with the non-personal nature of the call data.[86] UAS are distinguishable on this basis as well.

[26] However, *Greenwood* identifies another factor in the Court's *Katz* analyses: whether the information in question was divulged to the public

[83] *Id.* at 957 (internal citations omitted).

[84] U.S. v. Miller, 425 U.S. 435, 442 (1976).

[85] *See generally* Issie Lapowsky, *Facebook Lays Out Its Roadmap For Creating Internet-Connected Drones*, WIRED (Sept. 23, 2014, 1:07 PM), http://www.wired.com/2014/09/facebook-drones-2/, *archived at* http://perma.cc/C6LX-LJNN (explaining Facebook's plan for bringing Internet access to the world through drones).

[86] Smith v. Maryland, 442 U.S. 735, 743–45 (1979).

at large.[87] To be fair, that case also cited a "voluntary" disclosure of information to a third party—the trash collector—in expectation of services provided.[88] But it is not at all clear that the result rested on this relationship. The Court appeared just as concerned with the fact that the suspect's garbage was accessible to curious members of the public.[89] While commercial or private drones could conceivably be used to retrieve information a citizen sought to protect as secret—for instance, by monitoring electronic transmissions—it seems people are far more concerned with the images they might capture. In this, *Greenwood* is of little help and would suggest that any images taken of an individual on public roads would be subject to appropriation by law enforcement.[90]

[27] Finally, *Jones* suggests the Court is beginning to consider rethinking the third party doctrine in the context of the digital age. Sotomayor's concurrence explicitly states this,[91] and five of the justices would likely have found a Fourth Amendment violation based solely on *Katz's* "reasonable expectations" test.[92] The Court's narrow basis for its holding, however, kept the third-party doctrine alive for the time being.

[28] *Jones* may indeed suggest that the Supreme Court is open to breathing new life into the Fourth Amendment as technology continues to permit cheaper, more pervasive surveillance.[93] And in the context of digital information, at least one current Justice may be open to rethinking

[87] California v. Greenwood, 486 U.S. 35, 40–41 (1988).

[88] *Id.*

[89] *Id.*

[90] *See id.*

[91] United States v. Jones, 132 S. Ct. 945, 957 (2012).

[92] *Id.* at 954–64.

[93] *Id.* at 962–63.

(or eliminating) the third-party doctrine.[94] Nevertheless, at the moment, it appears that images legally collected by UAS would often be available for government access—at least so long as the contents of those images conveyed information revealed to the public.[95]

[29] If that is the case, one can reasonably expect that the third-party doctrine will influence regulatory approaches to commercial UAS at the state and local level. For example: the ACLU (a staunch proponent of, and lobbyist for, UAS regulation) is currently concerned largely with restricting government surveillance.[96] However, that may change—once private UAS assimilate into our airspace[97]—if law enforcement begins using the third-party doctrine as a loophole to retrieve data without probable cause or a warrant.[98] Granted, it may not be legal or profitable

[94] *Id.* at 957.

[95] *See generally* Carol Cratty, *FBI Uses Drones for Surveillance in U.S.*, CNN (June 20, 2013, 7:27 AM), http://www.cnn.com/2013/06/19/politics/fbi-drones/, *archived at* http://perma.cc/5J4T-99FF (stating that the FBI's policy on retaining images from drones is unclear).

[96] *See, e.g.*, Neema Singh Guliani, *Unchecked Government Drones? Not over My Backyard*, ACLU (Mar. 24, 2015, 3:23 PM), https://www.aclu.org/blog/speak-freely/unchecked-government-drones-not-over-my-backyard?redirect=blog/technology-and-liberty/unchecked-government-drones-not-over-my-backyard, *archived at* https://perma.cc/K698-AHKW?type=source.

[97] Because public entities dominate the domestic UAS scene for the moment, it is possible that the ACLU is simply focused on the more immediate issue. *See id.*

[98] At least one writer on the ACLU website has made this connection in the context of law enforcement use, condemning a North Dakota bill that would permit the use of evidence incidentally collected during an authorized government drone flight. *See* Allie Bohm, *Drone Legislation: What's Being Proposed in the States*, ACLU (Mar. 6, 2013, 3:15 PM) https://www.aclu.org/blog/free-future/drone-legislation-whats-being-proposed-states, *archived at* https://perma.cc/UQ5X-XPMT?type=source [hereinafter *Drone Legislation: What's Being Proposed in the States*] ("[T]here are also bills that take the low road: North Dakota's bill explicitly allows incidentally collected information to be introduced in court. So, if a drone on the way to fight a forest fire happens to record you

for a private entity to track a particular subject's every move. On the other hand, one can easily imagine that a private drone collecting images in an urban setting will happen to snap a photograph of a crime in progress. Under many states' existing schemes for UAS regulation, the government would be required to ignore or destroy such an image if it originated from a government drone—but *not* if it originated from a privately-operated drone.[99] Privacy advocates that have so rigorously promoted a higher standard for government surveillance will certainly want to eliminate this discrepancy.

B. The First Amendment

[30] The Fourth Amendment will not be the Constitution's only contribution to the debate over commercial UAS. Courts have read into the First Amendment a right—held not just by the press, but by private citizens—to information gathering.[100] Because the Supreme Court has yet to rule on the matter, however, the extent of behavior the First Amendment might protect is not entirely clear.

[31] The most recent cases discussing this "right to record" have centered largely on private citizens' recording of police activity.[101] This is

engaged in private activities, the police would not be required to delete that information and could actually use it in court against you, no warrant required—before or after the fact. This could create some dangerous incentives.").

[99] *See generally* Rich Williams, *2014 State Unmanned Aircraft Systems (UAS) Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 16, 2014), http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx, *archived at* https://perma.cc/ZL7X-QHV8?type=source (summarizing the current state legislation regarding UAS).

[100] *See, e.g.*, Glik v. Cunniffe, 655 F.3d 78, 83 (1st Cir. 2011); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000).

[101] *See, e.g.*, *Glik*, 655 F.3d at 83; *Smith*, 212 F.3d at 1333; Williamson v. Mills, 65 F.3d 155, 156 (11th Cir. 1995).

not surprising; police secrecy and police misconduct stir negative reactions from unease to revulsion. Moreover, the benefits of greater transparency in this area—such as protecting citizens from abuse, and holding police responsible for abusing their positions of power[102]—would seem to far outweigh any detriments.[103] Accordingly, several Circuit Courts of Appeal have held that private citizens have a First Amendment right to record law enforcement activities.[104]

[32] One of the more recent of these decisions is *Glik v. Cunniffe*.[105] In that case, plaintiff Simon Glik brought a § 1983 claim alleging that his First Amendment rights had been violated by his arresting officers.[106] Glik—happening on an arrest in progress—had begun filming the event when it appeared that the police were harming the arrestee and was subsequently arrested for violation of a wiretap statute.[107] The First Circuit held in Glik's favor, citing a slew of authority establishing his right to record the officers' actions.[108] Notably, the court also held that the right

[102] In addition, the recordings themselves are competent evidence for trial. *See* FED. R. EVID. 1001, 1002.

[103] *See, e.g.*, Steven A. Lautt, Note, *Sunlight Is Still the Best Disinfectant: The Case for A First Amendment Right to Record the Police*, 51 WASHBURN L.J. 349, 355 (2012) ("As a leading reason for their opposition to citizen-surveillance, police advocates have cited the concern that officers will hesitate in life-threatening situations for fear of their actions being caught on video. However, the more prevalent concern for police officers is the risk video monitoring poses to the substantial deference courts give officers in their official recounting of facts.").

[104] *See, e.g.*, *Glik*, 655 F.3d at 83; *Smith*, 212 F.3d at 1333.

[105] *Glik*, 655 F.3d at 83.

[106] *Id.* at 79.

[107] *Id.* at 79–80.

[108] *Id.* at 82–89.

was firmly established within its jurisdiction—as required by § 1983.[109] Finally, it established in clear language that the First Amendment protects not only the press's right to record, but that of individuals, as well. The court focused in particular on the location of the recording, noting that "Glik filmed the defendant police officers in the Boston Common, the oldest city park in the United States and the apotheosis of a public forum. In such traditional public spaces, the rights of the state to limit the exercise of First Amendment activity are 'sharply circumscribed.'"[110]

[33] The *Glik* court clarified that the right to record, like any First Amendment activity, is "subject to reasonable time, place, and manner restrictions."[111] Although it declined to explore these further, its holding is instructive in that it relies on *Perry Educ. Ass'n v. Perry Local Educators' Ass'n* for the proposition that states' ability to limit recording is "sharply circumscribed" in public.[112] *Perry*, a 1983 Supreme Court case, involved not recording but traditional speech activities.[113]

[34] Other circuits are consistent with *Glik* in recognizing a right to record police officers in public.[114] Although the *Glik* court mentioned two somewhat contrary decisions in the Third and Fourth circuits, these rested on the "clearly established" portion of the § 1983 analysis, not on whether

[109] *Id.* at 88.

[110] *Glik*, 655 F.3d at 84 (citing Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983)).

[111] *Id.* at 84.

[112] *Perry*, 460 U.S. at 45.

[113] *Id.* at 38–40.

[114] *See, e.g.*, Bowens v. Superintendant of Miami South Beach Police Dep't., 557 Fed. Appx. 857, 863 (11th Cir. 2014); *Smith*, 212 F.3d at 1333; Williamson v. Mills, 65 F.3d 155, 156 (11th Cir. 1995).

the constitutional right existed *per se*.[115] Moreover, *Kelly v. Borough of Carlisle* dealt with recording during a traffic stop—a situation the court distinguished as inherently dangerous.[116]

[35] Thus, most or all courts are in agreement in acknowledging the right to record police in public. Courts in most Circuits also agree that the right to record extends to matters of public concern.[117] However, there has been less agreement (and less guidance in general) on other circumstances in which the right to record will apply.[118]

---

[115] *Glik*, 655 F.3d at 85.

[116] *Id.* Further, in 2014, the First Circuit clarified that the right to record in a traffic stop, while not unqualified, is now "clearly established." Gericke v. Begin, 753 F.3d 1, 9 (1st Cir. 2014).

[117] *See Smith*, 212 F.3d at 1333 ("The First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest."); *see also* Iacobucci v. Boulter, No. Civ. A. 94-10531-PBS, 1997 WL 258494 at *6 (D. Mass, Mar. 26, 1997) (unpublished opinion) (finding that an independent reporter has a protected right under the First Amendment and state law to videotape public meetings); Fordyce v. City of Seattle, 55 F.3d 436, 439 (9th Cir. 1995) (recognizing a "First Amendment right to film matters of public interest"); Blackston v. Alabama, 30 F.3d 117, 120 (11th Cir. 1994) (finding that plaintiffs' interest in filming public meetings is protected by the First Amendment); *Williamson*, 65 F.3d at 159 (11th Cir. 1995) (reversing district court's grant of qualified immunity to a law enforcement officer who seized the film of and arrested a participant in a demonstration for photographing undercover officers); Thompson v. City of Clio, 765 F. Supp. 1066, 1070–72 (M.D. Ala. 1991) (finding that city council's ban on member's attempt to record proceedings regulated conduct protected by the First Amendment); Lambert v. Polk County, 723 F. Supp. 128, 133 (S.D. Iowa 1989) ("[I]t is not just news organizations . . . who have First Amendment rights to make and display videotapes of events...."); United States v. Hastings, 695 F.2d 1278, 1281 (11th Cir. 1983) (finding that the press generally has no right to information superior to that of the general public) (citing Nixon v. Warner Communications, Inc., 435 U.S. 589, 609 (1978)).

[118] *See, e.g.*, Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4. CAL. L. REV. CIR. 57, 63–64 (2013) (questioning whether the First Amendment right will apply with drone photography).

[36] How, then, will courts analyze the First Amendment rights of UAV operators? *Glik* appears to indicate that some existing precedent on "time, place, and manner" restrictions will enter into the analysis: the right to speak is at its strongest in public places, and so is the right to record.[119] However, other First Amendment principles are less susceptible to such a simple analogy. For example, an early step in First Amendment analyses is to determine the *type* of speech. This question is difficult to answer in the UAV context—taking a picture is taking a picture.[120] Similarly, true speech can be regulated in areas in which there probably remains a constitutional protection for information gathering. The Supreme Court has held it constitutionally permissible to restrict *speech* at airports,[121] but it would make little sense to prohibit *photography* in a place (1) with significant law enforcement presence, and (2) in which patrons have very little expectation of privacy. Precedent will not always be as useful as the court in *Glik* found it to be. Therefore, there is yet little guidance on what types of time, place, and manner restrictions will be constitutional in the UAV context.

[37] Ultimately, the extent of constitutional protections for UAV operators will boil down to a weighing of privacy against expression.[122] Seth Kreimer has identified one relevant principle of First Amendment law that might guide such an analysis:

---

[119] *Glik*, 655 F.3d at 84.

[120] One might examine the purposes of collecting an image: are they artistic? Journalistic? Scientific? That approach could work in limited circumstances—for example, vulgar purposes could constitutionally be proscribed.

[121] *See* Int'l Soc'y for Krishna Consciousness of Cal., Inc. v. City of L.A., 48 Cal. 4th 446, 460 (2010).

[122] *See* Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 392–93 (2011).

> [R]egulation must follow established legal rules that authoritatively recognize the scope of the privacy interest at stake and tailor the response to meet concerns of constitutional magnitude. Catchall statutes . . . do not meet this requirement. Nor do claims of street-level bureaucrats who maintain a right to discharge their duties in public without being recorded, nor those of private parties who seek to remove from the public domain images they have revealed to the public gaze. . . .
>
> Once we recognize that image capture is protected by principles of free expression, proposals to impose liability without observing the established limitations of privacy torts—either by common law innovation or by statute—raise serious constitutional questions.[123]

If Kreimer's observations are correct, lawmakers passing "drone" legislation may be faced with an ironic result: their laws may violate the First Amendment unless they more or less align with the existing legal systems they deemed inadequate.[124] Laws that restrict UAS capturing images of private property, for example, could fail (1) because of overbreadth and (2) because they fail to conform to established expectations of privacy.

[38] One more facet of First Amendment doctrine that deserves note is a preference for narrow holdings that will probably apply in circumstances involving UAS. In *Bartnicki v. Vopper*, the Supreme Court reaffirmed this approach: "[w]e continue to believe that the sensitivity and significance of the interests presented in clashes between [the] First Amendment and privacy rights counsel relying on limited principles that sweep no more

[123] *Id.* at 393, 398.

[124] *Id.* at 389–91.

broadly than the appropriate context of the instant case."[125]

[39] This preference could have a particularly deleterious effect on a burgeoning UAS industry. State laws that broadly violate the First Amendment, rather than being tested on their faces in the courts, could instead survive for years (with minor erosions). In the meantime, commercial drone users will surely avoid investing in "illegal" activities that may or may not be constitutionally protected—and insurers will avoid insuring them.

[40] It may seem odd to some that the right to take a picture would be protected by the First Amendment—after all, it is conduct with little content. But there are strong arguments for such a protection. People often take pictures in anticipation of disseminating them later.[126] And even if that is not the photographer's intention, she should not be deemed universally unworthy of First Amendment protections. The Court has stated free speech includes the freedom *not* to speak at all, and even "communications of one" inform later acts of speech.[127]

[41] UAS will be used to exercise freedom of speech in numerous—and worthwhile—ways. One obvious example is by the media: drones will soon be capable of performing every function a news helicopter can, and

[125] Bartnicki v. Vopper, 532 U.S. 514, 529 (2001) (quoting Fla. Star v. B.J.F., 491 U.S. 524, 532–33 (1989)).

[126] Kreimer, *supra* note 122, at 381 ("One might try to dissect the medium into its component acts of image acquisition, recording, and dissemination and conclude that recording is an unprotected 'act' without an audience. But this maneuver is as inappropriate as maintaining that the purchase of stationery or the application of ink to paper are 'acts' and therefore outside of the aegis of the First Amendment.").

[127] *Id.* at 378–79 ("Diaries of words or images need not communicate with outsiders to merit constitutional protection under the First Amendment. . . . Speech is protected not simply as a way of communicating with others, but as a means of defining the speaker's thoughts, intellect, and memories.").

more. But there will be other UAS uses tied highly to freedoms of expression, including some that we may not anticipate. One example is "drone art"—artwork created from images taken by UAVs.[128] NBC News sponsored the first "New York City Drone Film Festival" in March of this year.[129] People from landscape artists to Hollywood film producers will want to incorporate these aircraft in their media of expression.

[42] In the meantime, states' drone policies have already begun to violate First Amendment rights. The Texas Privacy Act may, in fact, have been designed to do just that: the law was proposed after a drone hobbyist discovered a slaughterhouse polluting a river with pig's blood.[130] In this sense, the Act (and others like it) could be construed as an effort to protect businesses' privacy from individuals under the guise of doing the reverse. Although the law may be struck down if challenged and although it creates exemptions for certain test sites,[131] Texas has proven that states may not be the most conscientious laboratories for developing drone legislation.

---

[128] *The Art of Drone Painting*, Center for the Study of the Drone, Bard College (Dec. 6, 2014), http://dronecenter.bard.edu/art-of-drone-painting/, *archived at* http://perma.cc/XS8S-A3FG.

[129] Organized for the first time in 2014, the festival was started by an enthusiast "with a desire to change the perceptions of drones." *New York City Drone Film Festival*, NBC NEWS, http://nycdronefilmfestival.com/, *archived at* http://perma.cc/YQ7L-PWKX (last visited Apr. 11, 2015); *New York Drone Film Festival Is Meant to 'Fight Stigma,' Creator Says*, NBC NEWS (Mar. 5, 2015, 12:30 PM), http://www.nbcnews.com/storyline/nyc-drone-film-festival/nyc-drone-film-festival-n318121, *archived at* http://perma.cc/DST3-BPRY.

[130] Laura Patty, *The Sky Is the Limit: Regulating The Next Generation of Privacy Invasion*, GOLDEN GATE U. L. REV. (2013), *available at* http://ggulawreview.org/2013/11/29/the-sky-is-the-limit-regulating-the-next-generation-of-privacy-invasion-2/, *archived at* http://perma.cc/JG26-HSBV ("Don't mess with the meatpacking lobby in Texas.").

[131] Tex. Gov't Code § 423.002 (2013).

C. Existing Privacy Protections

[43] Of course, a large number of existing state laws will also apply to the domestic use of drones. Flying UAVs at a low and/or unsafe altitude over private property could violate trespass laws.[132] Use a drone for snooping, and you could face liability under intrusion upon seclusion, stalking, harassment, or nuisance theories.[133] Distribute the images you obtained, and the list of laws you may have broken grows to include "public disclosure of private facts." [134] Intercepting data or communications could conceivably violate wiretap statutes.[135] Some privacy frameworks may require rewording to explicitly cover UAS; others will suffice as written.[136]

[44] Scholars have written in detail about the interaction between existing laws and UAS activity; for example, John Villasenor has published an article including an extensive and unbiased survey.[137] However, the *existing* framework of privacy protections will have little impact on the advent of commercial UAVs. UAVs used for benign information gathering will represent the vast majority of the commercial market,[138] and will not run afoul of existing privacy laws—provided that they remain within their permitted airspace. This Article therefore

[132] *See* Villasenor, *supra* note 5, at 499.

[133] *Id.* at 500–01.

[134] *Id.*

[135] *Id.* at 498.

[136] *See id.* at 499–500 (Arizona trespass statute likely applies to UAVs, whereas Oregon's and California's may not).

[137] *See* Villasenor, *supra* note 5, at 498–508. Readers who are interested in this topic are encouraged to consult John Villasenor's work.

[138] *See* Doering, *supra* note 26.

foregoes further coverage of the subject.

D. Proposed and Enacted "Drone Laws" at the State and Local Level

[45] In 2013, forty-three states proposed bills specifically regulating UAVs.[139] In 2014, that number grew and many of the bills were enacted.[140] As of the writing of this article, legislation has been passed in more than twenty of those states.[141]

[46] Most states' primary concern has been regulating law enforcement use of UAVs. Accordingly, most of the proposed bills in 2013—for example—would require a warrant for law enforcement to use a drone for surveillance of a suspect, subject to certain exceptions, including emergency situations.[142] A number of different approaches have emerged—for instance, legislation passed in Georgia permits surveillance only to investigate felonies, not misdemeanors.[143] Virginia has passed a two-year moratorium on all law enforcement use of UAVs.[144] A Nebraska bill prohibits law enforcement use—with or without a warrant—except in terrorism investigations.[145]

---

[139] *See Status of 2014 Domestic Drone Legislation*, *supra* note 18.

[140] *See 2014 State Unmanned Aircraft Systems (UAS) Legislation*, NAT'L CONF. STATE LEGIS. (Sept. 16, 2015), http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx, *archived at* http://perma.cc/6KEE-7T3F.

[141] *See, e.g.*, Williams, *supra* note 16.

[142] *See Drone Legislation: What's Being Proposed in the States?*, *supra* note 98 (surveying 2013 drone legislation).

[143] S.B. 200, 2013-14 Reg. Sess. (Ga. 2013).

[144] H.B. 2012, 2013 Sess. (Va. 2013).

[47] However, a number of states have already begun to consider private and commercial restrictions. A proposed bill in Missouri would ban using a drone to conduct video surveillance on any individual, or over private property, without consent.[146] In Washington, the House passed Bill 2178, which similarly prohibits persons from flying UAVs over private property without consent;[147] the Bill stalled in the Senate, but several of its policies were incorporated into another bill that *was* passed.[148] Wisconsin has approved a bill that would make it a misdemeanor to photograph, record, or otherwise observe an individual in any location in which the individual has a reasonable expectation of privacy.[149] A recent California bill would make it a trespass to fly a drone, without consent, over private property and "below the navigable airspace."[150] The Texas Privacy Act creates two separate misdemeanors: (1) non-consensual UAV imaging of private property, and (2) possessing or distributing an image so obtained.[151] And these are only some examples of legislation targeted at private or commercial UAS.

[48] Localities have also begun to restrict UAV flight, with much more

[145] L.B. 412, 103d Leg., 1st Sess. (Neb. 2013).

[146] H.B. 46, 97th Gen. Assemb., 1st Reg. Sess. (Mo. 2012).

[147] H.B. 2178, 63d Leg., 2014 Reg. Sess. (Wash. 2014).

[148] Ashley Stewart, *Bill Limiting Drone Use Passes House, Senate*, THE SEATTLE TIMES (Mar. 10, 2014, 4:54 PM), http://blogs.seattletimes.com/politicsnorthwest/2014/03/10/bill-limiting-drone-use-passes-house-sentate/, *archived at* http://perma.cc/B95J-7MQ2.

[149] S.B. 196, 2013-2014 Leg. (Wis. 2013).

[150] S.B. 142, 2014-2015 Leg. (Cal. 2015).

[151] *See* 2013 Tex. Gen. Laws 3691–94. In addition, the Act's definition of "image" includes sound and other forms of data. *See id.* at 3691.

peculiar results. Both St. Bonaficius, Minnesota and Evanston, Illinois have banned UAV flight within city limits.[152] Evanston's resolution exempts hobbyists from the ban, but St. Bonaficius's does not.[153] Of course, the most alarming solution proposed at the local level arises in Deer Trail, Colorado—the town that considered issuing "drone hunting" licenses.[154]

[49] So far, attempts to address commercial UAS at the state and local level have probably overreached at times. First, some likely run afoul of the First Amendment. Even if that is not the case, they fail to reflect a reasonable balance between privacy protections and the economic and social benefits of UAS.

[50] All the above examples have the potential, in their overreaching, to restrict the growth of the UAS industry, for several reasons. The first is simply that outlawing a technology, by definition, eliminates buyers from its market. But there's more to it. UAVs, by nature, will roam. They may pass through the airspace over multiple cities, or even multiple states. They may retrieve images of other jurisdictions without actually crossing overhead.[155] Operators will have to be aware of every law they might bump against; if those laws are unclear or too varied, they will be unable to calculate potential liability, and far less likely to invest in purchasing a drone.[156]

---

[152] *See* David Swanson, *All Drone Politics Is Local*, WAR IS A CRIME .ORG (Nov. 14, 2013), http://warisacrime.org/content/all-drone-politics-local, *archived at* http://perma.cc/FEW4-E8CY.

[153] *See id.*

[154] *See* Ryan Grenoble, *Done Hunting in Deer Trail, Colorado? Town Considers Bounty for Unmanned Aerial Vehicles*, HUFFINGTON POST (Jul. 17, 2013, 4:02 PM), http://www.huffingtonpost.com/2013/07/17/drone-hunting-deer-trail-colorado_n_3611806.html, *archived at* http://perma.cc/6ZE2-P4WP.

[155] *See* Villasenor, *supra* note 5, at 515.

[51] Operators will also want insurance from legal liability for their UAV operations. This could wind up being very expensive, and not just because uncertainty in the law will raise costs. Insurers are nothing if not cognizant of risk. The potential liability exposure of operating a UAV in some of the jurisdictions listed above would be massive. A commercial drone hovering in a single location could conceivably capture images of hundreds of individuals' private property. Neither an operator nor an insurer would want to take that risk in, say, Texas or Wisconsin.

E. Federal Sources of Regulation—The FAA

[52] The Federal Aviation Administration, or "FAA," is an arm of the Department of Transportation ("DOT").[157] Its primary mission is aviation safety.[158] The current organization has its origins in a 1958 act of

[156] For one person's anecdote on how regulations disappoint potential customers and spoil UAS deals, *see* Mike Francis, *Drone Company Says Ambiguity in Federal Regulations Keeps Customers on Sidelines*, OREGONLIVE (Apr. 3, 2014, 10:24 AM), http://www.oregonlive.com/business/index.ssf/2014/04/drone_company_says_ambiguity_i.html, *archived at* http://perma.cc/3EFG-FQPQ ("Stephen Burtt, the cofounder and CEO of Aerial Technology International, says his Clackamas-based company has answered many inquiries about its unmanned aerial systems—drones—from potential corporate customers. . . . [T]he conversations have been promising, with customers seeing the value of buying one of the company's drones to carry out tasks that currently require pilots or other workers. But then the corporate legal department gets involved. And the potential sale stalls. 'There's an incredible level of frustration' about the state of federal regulation of unmanned vehicles, he said. The slow rollout of regulations in this country means 'the rest of the world has much more developed markets' for the use of drones.").

[157] *See Our Administrations*, U.S. DEP'T TRANSP., http://www.dot.gov/administrations, *archived at* http://perma.cc/DD5W-Z5DF (last updated Mar. 10, 2015).

[158] *See Mission*, FED. AVIATION ADMIN., http://www.faa.gov/about/mission/, *archived at* http://perma.cc/B6DZ-KBPD (last modified Apr. 23, 2010, 9:37:40 AM) ("Our continuing mission is to provide the safest, most efficient aerospace system in the world.").

Congress creating a "Federal Aviation Agency"; the name change occurred in 1966, when the agency was incorporated into a newly-formed DOT.[159]

[53] The FAA's earliest predecessor entity was the Aeronautics Branch of the Department of Commerce, which was formed with the passing of the Air Commerce Act of 1926.[160] Before that time, the aviation industry had been stunted by the uncertainty of myriad state statutory and common law approaches.[161] Congress based its authority for regulating aviation on the Commerce Clause of the United States Constitution.[162]

[54] Those problems were remedied, and manned aircraft now enjoy a set of regulations, promulgated by the FAA, that is uniform throughout the United States. Consistent with its mission of fostering safety in the national airspace, the FAA promulgates generally-applicable rules regarding the design, maintenance, and operation of aircraft.[163] Because these rules were created with manned flight in mind, however, many of them do not or cannot apply to unmanned aircraft.[164] UAS have thrown a

[159] *See History*, FED. AVIATION ADMIN., http://www.faa.gov/about/history/brief_history/, *archived at* http://perma.cc/XR3W-WGL8 (last modified Feb. 19, 2015, 4:23:26 PM).

[160] *See id.*

[161] *See id.*

[162] *See* Timothy T. Takahashi, *Drones in the National Airspace*, 77 J. AIR L. & COM. 489, 518 (2012).

[163] *See, e.g.*, NAT'L RESEARCH COUNCIL, IMPROVING THE CONTINUED AIRWORTHINESS OF CIVIL AIRCRAFT: A STRATEGY FOR THE FAA'S AIRCRAFT CERTIFICATION SERVICE 12 (National Academy Press 1998).

[164] *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9549 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, 183).

wrench in the FAA's regulatory scheme—for example, lacking a cockpit, they cannot conform with the mechanical standards for cockpit doors.

[55] The FAA also classifies airspace according to a number of factors, including altitude ranges and proximity to airports.[165] Aircraft are subject to varying requirements depending on the airspace classes in which they operate.[166]

[56] The FAA has provided some guidance with respect to UAV operations. Direct line-of-sight to the aircraft is required at all times.[167] Drones may only be operated with a Certificate of Waiver or Authorization (hereinafter "COA") from the FAA, or through a Special Airworthiness Certificate-Experimental Category (hereinafter "SAC-EC").[168] COAs have been available for a number of years to public entities—such as law enforcement—that wish to operate a drone.[169] Only

[165] *See* Takahashi, *supra* note 162, at 507–09.

[166] *See id.* at 507.

[167] *See* Villasenor, *supra* note 5, at 472–73 ("Under the new law, public UAS operators have had access to expedited COAs since May 14, 2012. UAS under these authorizations must weigh no more than twenty-five pounds and be operated within the line of sight of the operator, less than 400 feet above the ground, and during daylight conditions.").

[168] *See Unmanned Aircraft Systems (UAS) Frequently Asked Questions*, FED. AVIATION ADMIN, https://www.faa.gov/uas/faq/, *archived at* https://perma.cc/89JY-WUFC (last modified Mar. 17, 2015, 11:02:52 AM).

[169] *See Fact Sheet—Unmanned Aircraft Systems (UAS)*, FED. AVIATION ADMIN (Jan. 6, 2014), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153, *archived at* https://perma.cc/VAA8-WBK2. For more detail on the process by which public entities receive authorization to operate UAVs, and on authorizations that have been granted, *see* Benjamin Kapnik, *Unmanned but Accelerating: Navigating the Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System*, 77 J. AIR L. & COM. 439, 445–46 (2012) ("To qualify for a certificate, the applicant must show the aircraft's response to losing communication with its operator, protocol if communication cannot be recovered, and that the unmanned aircraft can be

recently, though, did the FAA offer a blanket COA to private operators for which it had granted an "exemption." Before that, non-government UAS were authorized for experimental purposes only through the SAC-EC process.[170] The FAA has been sparing in granting exemptions to private or commercial operators.[171] As of April 21, 2015, it had granted only

contained within a proposed flight area. The applicant must provide documentation of: (1) the proposed operating area; (2) the manuals and checklists associated with the aircraft, including those for normal and emergency procedures; (3) training for relevant personnel; (4) evidence of completion of pilot licenses or other necessary certification; and (5) proof that the Federal Communications Commission (FCC) has approved the frequency of spectrum used to communicate with the aircraft. The typical COA is valid for two years. Although the FAA initially refused to divulge information about the COA applications and awards, in response to a lawsuit by the Electronic Frontier Foundation, the agency released a list of sixty-one entities that had sought licenses to operate unmanned aircraft in April 2012. Of those entities, only four applicants were disapproved, and forty-one of the licenses remained active. Entities with active licenses include universities, federal agencies, local police departments, and branches of the military.").

[170] *See Unmanned Aircraft (UAS) Certifications and Authorizations*, FED. AVIATION ADMIN, http://www.faa.gov/uas/certifications_authorizations/, *archived at* http://perma.cc/AW5R-37KG (last modified Dec. 27, 2013, 4:03:43 PM) ("For civil operation, applicants may obtain a Special Airworthiness Certificate, Experimental Category by demonstrating that their unmanned aircraft system can operate safely within an assigned flight test area and cause no harm to the public. Applicants must be able to describe how their system is designed, constructed and manufactured; including engineering processes, software development and control, configuration management, and quality assurance procedures used, along with how and where they intend to fly. If the FAA determines the project does not present an unreasonable safety risk, the local FAA Manufacturing Inspection District Office will issue a Special Airworthiness Certificate in the Experimental Category with operating limitations applicable to the particular UAS.").

[171] *See* Kellington, *supra* note 38, at 39–40 ("Even under FMRA's directive, FAA will *only* issue COAs for UAVs to *public organizations.* Commercial operators who wish to test or use UAVs must either find a public organizational sponsor that will accept complete responsibility for the craft and for compliance with the terms of a COA or obtain an experimental certificate. . . . FAA has issued only a handful of experimental certificates for very limited flight tests, demonstrations, and training. FAA states on its

207.[172]

[57] Until recently, a debate was quietly brewing over whether the FAA had the authority to regulate small UAVs. One judge had categorized a small UAV as a "model aircraft" and outside the FAA's purview.[173] Prior to this case, the FAA had *requested* that modelers adhere to certain guidelines, but it had not attempted to *regulate* models specifically.[174] Rather, the Academy of Model Aeronautics (hereinafter "AMA")—a national group of modeling enthusiasts—established standards for model aircraft flying.[175] The AMA generally requires that its members purchase liability insurance and comply with the FAA's recommendations.[176]

[58] Consistent with this scheme, Congress—in its 2012 "FAA Modernization and Reform Act" (hereinafter "FMRA")—exempted model

website that it will not issue experimental certificates for UAVs except in very limited circumstances").

[172] *See Section 333*, FED. AVIATION ADMIN., http://www.faa.gov/uas/legislative_programs/section_333/, *archived at* http://perma.cc/HRE4-HLT7.

[173] *See* Decisional Order at 7–8, Huerta v. Pirker, Docket No. CP-217 (N.T.S.B. Mar. 6, 2014), *available at* http://www.ntsb.gov/legal/alj/Documents/Pirker-CP-217.pdf, *archived at* http://perma.cc/YK59-EQDB.

[174] *See* R.J. VAN VUREN, FED. AVIATION ADMIN., ADVISORY CIRCULAR: MODEL AIRCRAFT OPERATING STANDARDS (1981), *available a*t http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf, *archived at* http://perma.cc/AQB7-J3MT.

[175] *See* ACAD. OF MODEL AERONAUTICS, NATIONAL MODEL AIRCRAFT SAFETY CODE (2014), *available at* http://www.modelaircraft.org/files/105.pdf, *archived at* http://perma.cc/4WT8-A9DP.

[176] *See Benefits of this Association*, ACAD. OF MODEL AERONAUTICS, http://www.modelaircraft.org/membership/membership/overview.aspx, *archived at* http://perma.cc/JHA2-CPZ4 (last visited Apr. 10, 2015).

aircraft from future regulation by the FAA, provided the models meet certain criteria.[177]

[59] Recently the FAA began asserting that its Federal Aviation Regulations (hereinafter "FARs")—which govern the operation of "aircraft"—also apply to model aircraft.[178] This led to a case that ultimately confirmed (for now) the scope of the FAA's control over all forms of UAS.[179] In *Huerta v. Pirker,* the FAA sought to fine a paid drone operator for allegedly unsafe operations.[180] At first, an administrative law judge determined that the UAS was a "model aircraft" and not within the FAA's regulatory purview.[181] If that interpretation had prevailed, it would have opened up the sky to small commercial drones. That case, however, was reversed on appeal to the National Transportation Safety Board.[182] The Board held that models are "aircraft," too—and that the FAA's safety regulations applied to UAS (whether drone or model) with equal force.[183]

---

[177] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95 § 336(a), 126 Stat. 11, 77 (2012) (codified as amended in scattered sections of 49 U.S.C.).

[178] *See* Interpretation of the Special Rule for Model Aircraft, 79 Fed. Reg. 36,172, 36,172 (June 25, 2014) (to be codified at 14 C.F.R. pt. 91). The FARs broadly define "aircraft" as "a device that is used for intended to be used for flight in the air." 14 C.F.R. § 1.1 (2014).

[179] *See* Opinion and Order at 12, Huerta v. Pirker, Docket No. CP-217 (N.T.S.B. Nov. 17, 2014) [hereinafter Pirker Opinion and Order], *available at* http://www.ntsb.gov/legal/alj/Documents/5730.pdf, *archived at* http://perma.cc/9EUN-VZ9D.

[180] *See id.* at 1–2; *see also* 14 C.F.R. § 91.13 (2014) (stating "[n]o person may operate an aircraft in a careless or reckless manner so as to endanger the life or property of another.").

[181] *See id.* at 3.

[182] *See id.* at 2, 12.

[183] *See id.* at 12.

[60] In June 2014, before *Pirker* was reversed on appeal, the FAA released a notice entitled "Interpretation of the Special Rule for Model Aircraft."[184] The FAA's position is consistent with the ultimate result in *Pirker:* it contends that model aircraft (and all UAS or drones) fall within the statutory definition of "aircraft" and thus are generally subject to at least some existing FAA regulations.[185]

[61] Thus, existing case law (supported by the FAA's stance) suggests that, whether or not a UAV is a "model" aircraft, it will be subject to certain *existing* FAA regulations. And, going forward, UAVs will only be "models" exempt from *future, targeted* regulation if they are flown for recreational purposes.[186] UAS that are used commercially would not meet that definition.[187] The FAA has clearly established its intent to regulate commercial UAS, whatever their size.

[62] One final lens for assessing the framework of developing drone regulation comes again from the FAA. In November 2013 the FAA released its "Roadmap for Integration of Civil Unmanned Aircraft Systems in the National Airspace."[188] The primary purpose of the Roadmap was to "align proposed FAA actions with Congressional mandates."[189]

---

[184] *See* Interpretation of the Special Rule for Model Aircraft, 79 Fed. Reg. at 36,172.

[185] *See id.* at 36,173.

[186] *See id.* at 36,173–74.

[187] *See id.* at 36,174.

[188] *See* FED. AVIATION ADMIN., INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS IN THE NATIONAL AIRSPACE SYSTEMS (NAS) ROADMAP i (1st ed. 2013) [hereinafter ROADMAP], *available at* http://www.faa.gov/uas/media/uas_roadmap_2013.pdf, *archived at* http://perma.cc/4XB3-F3HR.

[189] *Id.* at i.

[63] The FAA's Roadmap did little from a practical perspective other than arrange six mandated test-sites for UAS research and operation.[190] The remainder of the document discussed the unique safety concerns posed by UAVs' presence in our crowed national airspace.[191] Principal among these is the need to develop "sense and avoid" technologies.[192] However, the Roadmap did propose an instructive timeline for integrating drones. The timeline is quite conservative: the FAA plans to continue accommodating UAVs on a case-by-case basis.[193] The following two steps—"integration" and "evolution"—are also expected to take about five years each.[194]

[64] Although (as discussed *infra*) the FAA has since taken steps to integrate small UAS into the national airspace, its Roadmap—which presumably still applies to larger drones—has faced criticism. The Association for Unmanned Vehicle Systems International ("AVUSI") sent a letter to the FAA, noting "AUVSI's economic impact study found that, in the first decade following integration, the UAS industry will create more than 100,000 jobs and $82 billion in economic impact. However, each day that integration is delayed will lead to $27 million in lost economic impact."[195]

---

[190] *See id.* at 37.

[191] *See id.* at 12.

[192] *See id.* at 28.

[193] *See* ROADMAP, *supra* note 188, at 21–22. Notably, however—if the FAA's proposed rules for small UAS are adopted—the case-by-case inquiry will apply only to larger drones.

[194] *See id.* at 6, 21.

[195] Letter from Michael Toscano, President & CEO, Ass'n for Unmanned Vehicle Sys. Int'l, to Michael Huerta, Administrator, Fed. Aviation Admin. (Jan. 27, 2014), *available at* http://higherlogicdownload.s3.amazonaws.com/AUVSI/f28f661a-e248-4687-b21d-

[65] It is difficult to tell what effect the FAA's conservative timeline might have on developing state regulations of civil UAS. A longer, slower process might eliminate some of the urgency to legislate. On the other hand, states will apparently have abundant time to do so—and without drones in our skies, it's unlikely that people will warm up to their benefits.

[66] There is one area in which the FAA has taken reasonable preliminary steps towards integration: small UAS. On February 15, 2015, the FAA proposed a framework of regulations governing small UAS.[196] The regulations have not yet taken effect; rather, the FAA has solicited public commentary through April 24, 2015.[197] However, the proposed rules would exempt UAS meeting certain qualifications from the FAA's case-by-case approval system.[198] Under the FAA's proposed rules, UAS that weigh less than fifty-five pounds could be flown by licensed "operators" during daylight hours at altitudes less than 500 feet.[199] While line-of-sight operation would still be required under the proposed regulations, this is a significant step forward for the commercial use of small UAS in the United States. Unfortunately, in certain states that have passed privacy laws restricting private UAS use, the FAA's action may mean little: even if aircraft meet the federal safety standards, it will be virtually impossible to fly them lawfully where unauthorized photography

34342433abdb/UploadedFiles/1%2027%2014%20Letter%20on%20sUAS%20NPRM%20Delay.pdf, *archived at* http://perma.cc/R8YP-6HQV.

[196] *See* Press Release, Fed. Aviation Admin., DOT and FAA Propose New Rules for Small Unmanned Aircraft Systems (Feb. 15, 2015), *available at* http://www.faa.gov/news/press_releases/news_story.cfm?newsId=18295, *archived at* http://perma.cc/9SZ3-C4MB.

[197] *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. at 9544.

[198] See *id.* at 9579.

[199] *See id.* at 9576.

by UAS is prohibited.

[67] Much as states have, Congress has largely concerned itself with protections against law enforcement invasions of privacy.[200] One recurring bill, however, has included civil aircraft within its orbit. The "Drone Aircraft Privacy and Transparency Act of 2015" would, among other things, require *any* UAS seeking authorization to provide a "data collection statement" indicating the focus and purpose of its image-gathering.[201] It would also instruct the Secretary of Transportation to conduct a UAS privacy study and prepare a report.[202] While transparency in UAS operations might assuage privacy concerns, the administrative costs of such a nationwide program are unclear. The Act also creates a private right of action, which includes an attorney's fee provision and could have significant economic impact.[203]

IV. HOW SHOULD LEGISLATURES ADDRESS PRIVACY?

[68] In the broadest sense, there are three possible approaches to dealing with the privacy concerns that drones raise: (1) wait and see, (2) adopt a federalist system of regulation, or (3) enact a federal statute.[204] Each of these systems has its merits. Below, the arguments for and against the three regulatory schemes are outlined. It is ultimately suggested that the best course of action would be to adopt a carefully constructed federal privacy act governing drones. Such an act might

[200] *See, e.g.*, Preserving Freedom from Unwanted Surveillance Act of 2013, H.R. 972, 113th Cong. (1st Sess. 2013).

[201] Drone Aircraft Privacy and Transparency Act of 2015, S. 635, 114th Cong. (1st Sess. 2015).

[202] *See id.* at § 337(a), (b).

[203] *See id.* at § 4(d).

[204] Of course, combinations of these are always an option as well.

commission a study, or perhaps propose a baseline of privacy protections, while also ensuring that states cannot legislate so as to create a *de facto* ban on UAS over private property.[205]

A. The Case for Inaction

[69] The case for waiting on UAV legislation appears to be the least favorite among academics,[206] although it pops up from time to time in the news. Its arguments are not without merit. The UAV industry is in its infancy. It is impossible to predict all of its privacy implications, and therefore enormously difficult to draft conscientious laws that strike the proper balance between privacy and progress.[207] Smartphones have already given us a society with ubiquitous, ambulatory cameras, doing more to promote civil "surveillance" than drones are likely to do for some years to come. They convey various kinds of personal data to third parties, rendering it accessible by the government to search or introduce at trial. Yet few would argue we should outlaw cell phones in the name of privacy. The legislation that states have proposed so far has been similarly overbroad, prohibiting far more activity than required to protect privacy interests.

[205] Congress would have to be particularly mindful that any privacy protections do not restrict industry growth; the goal would be to assuage the concerns that have led states to impose harsher restrictions.

[206] One reason for this, I expect, may simply be the fact that an article prophesying impending doom is more attractive to publishers than an article suggesting that everything is probably fine.

[207] *See* Villasenor, *supra* note 5, at 461 ("[W]hen drafting new laws it is critical to adopt a balanced approach that recognizes the inherent difficulty of predicting the future of any rapidly changing technology. In the early days of the Internet and mobile phones, it would have been nearly impossible to accurately foresee all of the uses—both positive and otherwise—to which these technologies have been applied. It is similarly difficult today to predict exactly how UAS will be used—or even what they will look like—in the coming decades. Although unmanned aircraft pose real and increasingly well recognized privacy concerns, they also offer real and much less widely appreciated benefits.").

[70] Moreover, existing laws already provide a framework for restricting many improper invasions of privacy by UAS.[208] It would be more reasonable, and less likely to violate the First Amendment right to record, if states focused on adjusting existing laws to cover UAS. This way, states would limit only as much UAS activity as necessary to conform to existing privacy expectations.[209]

[71] Perhaps the most conclusive argument against the "wait and see" option is simply that the ship may have already sailed. At least forty-three states have proposed drone bills, and laws are on the books in at least twenty of them. There might still be hope that states will be more open to commercial applications, as only a quarter or so of states have specifically addressed private use.[210] It seems likely, however, that more states will take up that cause as it becomes more pressing.[211] For example, many states that addressed only public surveillance forbade the government from storing information collected inadvertently, or from using in court information about anyone other than the subject of the warrant.[212] Presumably those states will want to consider drafting similar restrictions for information collected by third-party UAVs.

[72] Another potential problem with such an approach is that, in all

[208] *See, e.g.*, *id.* at 498.

[209] However, this approach—despite reflecting a more reasonable balancing of interests—would not make the legal system any less varied or unpredictable. There are variations between states' existing privacy laws, and there will be variations between the courts' applications of those laws to UAVs. A uniform system would provide better notice of the standard to everyone, and would better enable development.

[210] *See supra* Part III.D.

[211] *See supra* Part III.D.

[212] *See Drone Legislation: What's Being Proposed in the States?*, *supra* note 98 (Massachusetts and Rhode Island are two examples).

likelihood, it will be very difficult to enforce existing privacy laws against improper actors without at least some drone-specific rules on the books. UAVs can be light, quiet, and virtually unnoticeable. They can observe from angles one normally would not expect, and see over walls and on rooftops. People who are illegally observed by UAS—for example, in violation of a "Peeping Tom" statute—may never know their rights have been violated, unless government imposes some restrictions.[213]

B. Drone Federalism

[73] There are also several arguments in favor of leaving commercial drone regulation largely in the hands of the states. The technology is new, and state experimentation might lead to a better result than a federal

[213] On the other hand, UAS-specific regulations could be just as difficult to enforce against private individuals as current privacy laws, conveying no benefit while also having a deleterious effect on legitimate business uses for UAVs. Companies that have gone to the expense of hiring a trained and licensed drone "operator" will presumably avoid actions that could subject them to civil or criminal liability. *See, e.g.*, Gregory S. McNeal, *FAA Has Commercial Drone Regulation Backwards*, FORBES (July 1, 2014, 4:32 PM), http://www.forbes.com/sites/gregorymcneal/2014/07/01/faa-struggling-to-deal-with-drones-now-going-after-realtors-and-farmers/, *archived at* http://perma.cc/7YED-GBW7 ("When a realtor or farmer uses a piece of equipment for commercial purposes their livelihood and businesses are on the line, [creating] clear incentives for safe operation (not to mention big insurance policies). They aren't going to fly irresponsibly and push the limits of their equipment because they are working with a clear purpose in mind."). On the other hand, it will be difficult to regulate the behavior of an average individual who bought a drone at the hobby store. Consider the recent White House incident, in which a drunken government worker accidentally breached some of the most heavily regulated airspace in the country. *See* Michael D. Shear & Michael S. Schmidt, *White House Drone Crash Described as a U.S. Worker's Drunken Lark*, N.Y. TIMES, Jan. 28, 2015, at A15, *available at* http://www.nytimes.com/2015/01/28/us/white-house-drone.html, *archived at* http://perma.cc/L6DA-XCJ5; Charlotte McCoy, *AMA Reacts to President Obama: More Regulation Wouldn't Have Prevented White House "Drone" Incident*, AMA GOV'T RELATIONS BLOG (Jan. 28, 2015), http://amablog.modelaircraft.org/amagov/2015/01/28/ama-reacts-to-president-obama-more-regulation-wouldnt-have-prevented-white-house-drone-incident/, *archived at* http://perma.cc/Z7SJ-959D.

"statute of first impression," so to speak.[214] Privacy—particularly outside of law enforcement contexts—has traditionally been a product of state and common law.[215]

[74] Margot Kaminski has made a compelling case for drone federalism, contending that states are better suited to address the "complex space" between the privacy and First Amendment rights at stake.[216] Kaminski argues that because federal legislation is more costly, more time consuming to enact, and more likely to be struck down as unconstitutional, states are a better laboratory for experimenting with approaches to commercial and private UAS regulation.[217] Moreover, state legislatures are capable of tailoring protections to meet new technologies according to their citizens' particular needs—for example, it should come of no surprise that California is one of a few states to pass an anti-paparazzi law.[218]

[75] Another argument made in favor of drone federalism (and privacy federalism in general) is that it is difficult for a single federal law to foresee each varied situation that may arise in the future.[219]

[76] It is possible that a pure federalism model would work well if—as is probably the case for less-controversial areas of the law—states cautiously tested the waters of restrictions on civil/commercial drones. Unfortunately, that does not appear to be the case here; they are diving

[214] *See* Kaminski, *supra* note 118, at 65.

[215] *See id.* at 66.

[216] *See id.* at 59.

[217] *See id.* at 64.

[218] *See id.* at 66.

[219] *See* Kaminski, *supra* note 118, at 461.

straight in.[220] The specter of drone warfare and robotic monitoring has wrought enough damage on drones' image that, by the time the FAA fully integrates private UAS in the national airspace, it may be impossible in a significant number of states to operate one without risking civil or criminal liability.[221] As mentioned earlier, as long as the third-party doctrine remains viable, the incentive for states to bring civil drone restrictions up to speed with moratoria on government surveillance will be great.[222]

[77] The states have also done little to demonstrate that they are concerned with the "complex space" between the First Amendment and privacy. The Texas Privacy Act, enacted in response to a drone's discovery of environmental violations, arguably violates the First Amendment outright. The cattle industry has sponsored bills in several states forbidding the recording of farmland.[223] Some states, by prohibiting flights over private property, appear to be straining to reach as much conduct as existing First Amendment precedent could possibly allow.

[78] Moreover, the Supreme Court's preference against issuing broad holdings when privacy and the First Amendment collide suggests that even some unconstitutional attempts are unlikely to be overturned in one fell swoop. Instead, courts might invalidate statutes on particular cases' facts. The result could be that unconstitutional laws persist for some time, continuing to infringe on First Amendment rights, eroding rather than being overturned.

---

[220] *See generally supra* Section III.D.

[221] *See* Villasenor, *supra* note 5, at 500–01.

[222] *See* Kaminski, *supra* note 118, at 66 (noting that one qualification, in order for drone federalism to function, is that "Congress must legislatively close the trap door that is the third-party . . . doctrine").

[223] *See id.* at 63 (noting that the cattle industry has been sponsoring bills that criminalize video recording on farms).

[79] Finally, of the three possible approaches, drone federalism would result in the greatest level of interstate variation and legal uncertainty. The aviation industry benefited from a consistent federal approach in 1926, and would again today, to the extent possible.[224]

C. Federal Regulation of Civil Drones and Privacy

[80] Even if privacy is traditionally within the states' domain, Congress also has a pedigree of privacy laws. Existing federal privacy laws are sectoral, carving out a particular privacy issue; several answer questions about the relationship between privacy and technology. For example, federal laws address telephone and electronic communications, [225] standards for the electronic exchange of health care information,[226] and the privacy of children's personal information online.[227] An act outlining baseline privacy policies for commercial UAS would not be out of place on such a list.[228]

[81] In addition, Congress' passing of the FMRA could suggest a

[224] Interestingly, today's argument that privacy is in states' domain mirrors concerns in 1926 that federal regulation of safety overreached.

[225] *See generally* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No.99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C §§ 2510–22 (2012)).

[226] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 § 261, 110 Stat. 1936, 2021 (codified as amended in scattered sections of 42 U.S.C.)

[227] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501(6), 6502(a)(1) (2012).

[228] Because aircrafts are so closely linked with interstate commerce (especially aircraft collecting and broadcasting data), I assume, for the purposes of this article, that a federal legislative scheme would be permissible under the Commerce Clause.

greater appreciation for the social and economic benefits of commercial UAV operations than many states currently have. The FMRA predicated the FAA's continuing funding on efforts to integrate drones into the national airspace.[229] The impetus is there for bipartisan support of a drone-friendly Act: having invested in the UAS industry's economic future, it is unlikely Congress would enjoy seeing the market flounder on state laws (once the FAA lives up to its part of the bargain).

[82] Finally, that federal legislation is more costly and often requires greater deliberation may in fact translate into better results than those currently being achieved by the states. While the extent of the First Amendment right to record is far from clear, Congress could establish baseline privacy-related rules that would prevent an act from being categorically stricken. And some privacy interests can be vindicated without implicating the First Amendment at all, as by enacting transparency requirements.[230]

D. The Potential Contents of a Federal Drone Act

[83] Congress's goals in drafting privacy rules that would govern commercial UAS should include (in no particular order):

1. Providing the clearest possible guidance to potential UAS manufacturers, operators, and insurers;
2. To the extent possible, establishing uniformity in permissible commercial or private UAS activities;
3. Facilitating commerce through enabling the expansion of beneficial UAS activities;

[229] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95 § 216, 126 Stat. 11 (2012).

[230] *See* Drone Aircraft Privacy and Transparency Act of 2015, S. 635, 114th Cong. (1st Sess. 2015). (But note that the Act's purview reaches far beyond transparency.)

4. Preventing usurpation by states of UAV operators' First Amendment right to information gathering;
5. Avoiding usurpation (to the extent possible) of states' traditional prerogatives regarding privacy rights;
6. Protecting individuals' reasonable expectations of privacy from unwanted recording; and
7. Avoiding Constitutional overreach.

[84] Transparency requirements are already being considered by Congress.[231] Transparency in UAV operations—if the actual requirements were crafted to avoid administrative costs—could feasibly serve each of the above-listed goals. For instance, anyone seeking to operate a UAV in the national airspace could be required to provide a "data collection statement" detailing (1) the information to be gathered, and (2) the information's intended use.[232] Companies that receive a grant of authorization for a particular model and purpose could also be permitted to avoid reapplying, as long as new models were used for the same activities. By making information about UAS operators available to the public, the government could assuage some of the same privacy concerns as would consent requirements (but without running afoul of the First Amendment). And exemptions could be made for certain categories of aircraft.[233]

[85] Privacy protections beyond that baseline become trickier. Congress *could* follow the lead of some states and prohibit surveillance of individuals in violation of reasonable expectations of privacy. This would certainly serve goal #6, and it likely avoids butting up against the First Amendment (goal #7). The standard it sets, however, is vague and might

[231] *See id.*

[232] *Id.* at § 339(a)–(b).

[233] The FAA has already proposed a similar scheme in its safety regulations; there is no reason that privacy regulations could not also be crafted differently to address different classes of technology. *See* NPRM, *supra* n. 8 (considering relaxed regulations for aircraft weighing under 4.4 lbs).

vary from state to state—hindering goals #1 and 2. A limited "anti-paparazzi" provision might work better. It could prohibit the targeted collection, or the transmission in interstate commerce, of certain types of private information or images—obscene photographs and the like.

[86] In order to avoid usurping states' ability to create their own privacy standards (goal #5), Congress could expressly disclaim any intent to occupy fields outside of drone-specific regulation.[234]

[87] Finally, Congress should exercise care in determining whether and how a federal Drone Act might preempt state law. While a broadly preemptive federal privacy statute would be best if market growth and efficiency were the only concern, such an approach could have several unfortunate consequences. First, broad preemption would extinguish states' abilities to respond to realistic, emerging privacy concerns not addressed federally.[235] Second, it would virtually ensure that federal rules will become dated or "ossified" as technology improves.[236] To address these concerns, Congress could put a time limit on its rules, or employ a single, narrowly preemptive ceiling. For example, it could establish that UAVs legally flying in navigable airspace cannot be prohibited from (1) navigating over private property or (2) recording video or images for purposes not that will not implicate privacy concerns.

[88] Congress has the will, resources, and impetus to create a baseline of federal privacy law governing civil drone use. It has a history of passing bold legislation for the betterment of the aviation industry. It has already mandated that the FAA begin ushering in a profitable, beneficial system for UAS operations. Federal guidance on civil drone use might

[234] For example, "nothing contained within this Act shall be construed to change the operation of state laws, existing or forthcoming . . . ."

[235] *See* Kaminski, *supra* note 118, at 64–66. On the other hand, states would remain free to rework existing privacy laws so that UAVs fall within their scope.

[236] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J 902, 927–28 (2009).

assuage states' concerns about invasion of privacy, and—better still—foster a system that welcomes interaction between the two levels of government, simultaneously enabling a valuable industry and protecting First Amendment rights.

IV. CONCLUSION

[89] It will take time for the FAA to achieve meaningful integration of commercial drones into the public airspace.[237] In the meantime, the states are ramping up privacy protections that ignore the benefits of unmanned aircraft, and infringe on First Amendment rights, in favor of privacy interests that may, in fact, be negligible.[238] This could spell problems for the future of drones in the United States—especially when the FAA's conservative approach to safety regulations already has politicians concerned about losing our edge over foreign competitors.[239] Privacy advocates' attitudes stem from fears that—in many cases—exhibit a misunderstanding of drones' profitable uses (and of the burdensome task of integrating drones in our airspace).[240] If states continue to pass laws

[237] *See generally* FAA Modernization and Reform Act of 2012, Pub, L. No. 112-95, 126 Stat. 11 (setting staggered annual and continuing deadlines for the act's integration, e.g., certain provisions of the NextGen project requiring an annual update on the progress of project implementation).

[238] *See* Kaminski, *supra* note 118, at 57–61.

[239] *See* Elizabeth Tennyson, *Hearing Reveals FAA Behind on NextGen, UAS, Consolidation*, AOPA (Feb. 6, 2014), http://www.aopa.org/News-and-Video/All-News/2014/February/06/FAA-behind-on-NextGen-UAS-and-consolidation-hearing-reveals.aspx ("Rep. Bill Shuster, chairman of the House Transportation and Infrastructure Committee, warned, '[t]he aviation industry was invented in America, and we continue to be the world leader in the airline industry and in aviation manufacturing. But if we're not careful and proactive, we could lose our position as the global leader in aviation, just as we've fallen behind in other important industries.'").

[240] *See supra* Part I. Also, the recent advent of weaponized drones for use in overseas warfare contributes to these fears, but has no justifiable connection to policy-making in a commercial context.

restricting commercial drones, Congress should consider enacting legislation to preserve a minimum of protection for *both* privacy interests and UAS' legitimate right-of-way.