2012

Drone Federalism: Civilian Drones and the Things They Carry

Margot E. Kaminski
University of Colorado Law School

California Law Review Circuit

VOL. 4 MAY 2013

Drone Federalism: Civilian Drones and the Things They Carry

Margot E. Kaminski*

ABSTRACT:

Civilian drones are scheduled to be permitted in the national airspace as early as 2015. Many think Congress should establish the necessary nationwide regulations to govern both law enforcement and civilian drone use. That thinking, however, is wrong. This Essay suggests drone federalism instead: a state-based approach to privacy regulation that governs drone use by civilians, drawing on states' experience regulating other forms of civilian-on-civilian surveillance. This approach will allow necessary experimentation in how to best balance privacy concerns against First Amendment rights in the imminent era of drone-use democratization. This Essay closes by providing some guidance to states as to the potential axes of drone-related privacy regulations.

INTRODUCTION

Civilians will fly drones in the national airspace soon, if Congress has its way.[1] Drones can carry a wide array of privacy-invading technologies, from

* Executive Director of the Information Society Project, Research Scholar, and Lecturer in Law at Yale Law School. Many thanks to Jack Balkin, Kevin Bankston, M. Ryan Calo, Catherine Crump, Joseph Lorenzo Hall, Christina Mulligan, and John Villasenor for their helpful comments.

1. FAA Modernization and Reform Act of 2012, H.R. 658, 112th Cong. (2012).

cameras to heat sensors to sensors that detect movement to odor detectors that can sniff the air.[2] Drones are also cheap to own and operate, compared to manned aircraft.[3]

States, fearing dragnet surveillance, have started examining gaps in privacy law.[4] Their fears are well-founded; a Seattle woman recently reported a drone hovering over her yard and outside her third-story window.[5] At the time of this Essay's writing, over thirty states are actively considering drone-related legislation, and the federal government has proposed several bills, one of which likely preempts most state regulation.[6] This legislative surge demands a study of whether drone privacy law is better handled by the federal government, or by the states.

The federal government has a history of regulating law enforcement surveillance through the federal wiretap statute, which could be updated to govern other law enforcement uses of drones. An updated federal statute could therefore provide the floor for state regulation of law enforcement drone use, and the more limited subject matter of remote wiretapping by private parties.[7] However, governing civilian drone use on other matters, particularly video and

---

2. *See Unmanned Aerial Vehicles Support Border Security* CUSTOMS & BORDER PROTECTION TODAY (July/Aug. 2004), http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml*; see also* H.B. 912, 83d Leg. (Tex. 2013) § 423.001 ("In this chapter, "image" means any capturing of sound waves, thermal, infrared, ultraviolet, visible light, or other electromagnetic waves, odor, or other conditions existing on or about real property or an individual located on that property.").

3. *See, e.g.*, Chris Anderson, *How I Accidentally Kickstarted the Domestic Drone Boom*, WIRED (June 22, 2012), http://www.wired.com/dangerroom/2012/06/ff_drones/all/ (explaining that toy drones with the same capabilities as military drones sell "sometimes for less than $1,000" and hobbyist drones are "dirt-cheap")*; see also* Dan Ashley, *Popularity of Drones Raises Privacy Concerns*, ABC NEWS.COM (June 18, 2012), http://abclocal.go.com/kgo/story?section=news/assignment_7&id=8706281 (quoting drone enthusiast Mark Harrison as saying of hobbyist drones that "[e]ven a couple of years ago, this would be like a $10,000, $20,000 project and now [having] it be like $500, $600, as cheap as a smart phone, as cheap as a laptop computer, makes it pretty feasible").

4. M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 (2011), http://www.stanfordlawreview.org/online/drone-privacy-catalyst.

5. Rebecca J. Rosen, *So This is How it Begins: Guy Refuses to Stop Drone-Spying on Seattle Woman*, ATLANTIC (May 13, 2013), http://www.theatlantic.com/technology/archive/2013/05/so-this-is-how-it-begins-guy-refuses-to-stop-drone-spying-on-seattle-woman/275769/ (quoting the woman: "I initially mistook its noisy buzzing for a weed-whacker on this warm spring day. After several minutes, I looked out my third-story window to see a drone hovering a few feet away").

6. Allie Bohm, *Status of Domestic Drone Legislation in the States*, ACLU (Feb. 15, 2013 12:21 PM), http://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states.

7. Civilian-on-civilian wiretapping is governed by the federal Electronic Communications Privacy Act (EPCA). Because it contains a one-party consent requirement and exceptions where one party does not have a reasonable expectation of privacy to the recording, ECPA's application to private parties is unlikely to be a central concern of drone regulation. However, it might be triggered by private use of cell site simulators, or "StingRays," which intercept calls by tricking phones into thinking they are cellular towers. Cell site simulators could be carried by drones. *See, e.g.*, Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST (Mar. 27, 2013), http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html.

image capture, will be far more complex, and will more closely resemble the regulation of subject matter traditionally covered by the states.

Like all laws governing videos by private actors, drone surveillance laws will exist between a privacy floor and a First Amendment ceiling. For now, I argue, this complex space of privacy regulation is best left to the states.

I.
DRONE PRIVACY REGULATIONS

There are, broadly speaking, two subjects of drone privacy regulation: law enforcement drone use and civilian drone use.[8] Most advocates and academics have focused on establishing privacy regulations to govern law enforcement drone use.[9] This task is worthy of immediate attention. The FAA already permits law enforcement drone use, where it does not yet permit commercial private drone use.[10] A number of state and federal bills thus propose warrant requirements for drone surveillance by law enforcement.[11]

The federal government could regulate law enforcement drone use as it has historically regulated other law enforcement behavior, by providing a floor for state laws.[12] Federal legislation already governs law enforcement use of wiretaps and pen registers.[13] Drone surveillance is likely to additionally involve video surveillance, location tracking, and/or facial recognition, among other possible technologies. Thus federal legislation governing law enforcement surveillance could be expanded to govern location tracking, video surveillance, and the use of facial recognition software by law enforcement.[14]

---

8. *See* John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J. L. & PUB. POL. 457 (2013).

9. *See* Paul McBride, *Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations*, 74 J. AIR. L. & COM. 627 (2009); Travis Dunlap, *We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search*, 51 S. TEX. L. REV. 173 (2009).

10. *See* FAA Modernization and Reform Act of 2012 § 334(c), H.R. 658, 112th Cong. (2012).

11. *See* Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. (2013) (requiring a warrant or court order for law enforcement drone surveillance, with exceptions for border usage, consent, and emergencies); Preserving Freedom from Unwanted Drone Surveillance Act of 2012, S. 3287, 112th Cong. (2012) (requiring a warrant, except for border patrolling, exigent circumstances, and high risk of terrorist attack); Drone Aircraft Privacy and Transparency Act of 2013, H.R. 6676, 112th Cong. (2012) (requiring a warrant except in exigent circumstances, including imminent danger of death or a high risk of terrorist attack); *see also* Allie Bohm, *Drone Legislation: What's Being Proposed in the States?*, ACLU (Mar. 6 2013, 3:15 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/drone-legislation-whats-being-proposed-states (listing states considering drone legislation requiring a probable cause warrant: Arizona, California, Florida, Georgia, Idaho, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, Montana, New Hampshire, New Mexico, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Washington, and Wyoming).

12. *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2522).

13. *Id.*

14. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012). Recently, the House considered proposed amendments to ECPA to expand its coverage to include geolocation data retained

Regulating law enforcement drone use poses few countervailing dangers from legislating thoughtlessly or in haste; such legislation would implicate Fourth Amendment rights rather than First Amendment rights, so the worst case scenario is that such legislation might eventually be found by courts not to protect enough privacy.[15]

The more interesting and difficult privacy puzzle arises from drone use by private—not public—actors. Regulating civilian drone use will be treacherous, as such regulation potentially threatens First Amendment rights. Because of that threat, civilian drone regulation may get overturned, as courts sort out the scope of those First Amendment rights. Regulating civilian drone use on the federal level thus risks being unconstitutional or, barring that, unstable.

Several states are considering banning civilian drone photography, or more broadly, civilian drone use.[16] The proposed Texas Privacy Act, H.B. 912, bans drone photography without the consent of the property owner on whose property the image is taken, and at the time of this Essay's writing, has passed the Texas House and is up for debate in the state Senate.[17] Two proposed federal bills restrict the gathering of images and other information by civilians.[18] One of these federal bills can be read to preempt state regulation of drone flights between states.[19] This Essay argues that preemption of state drone regulation would be a mistake.

---

by communications providers. *See* Kevin Bankston, *Today's Other EPCA Reform News: Location Privacy Hearing in the House*, CENTER FOR DEMOCRACY & TECHNOLOGY (Apr. 25, 2013), https://www.cdt.org/blogs/kevin-bankston/2504today%E2%80%99s-other-ecpa-reform-news-location-privacy-hearing-house.

15. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

16. H.B. 46, 97th Gen. Assemb., Reg. Sess. (Mo. 2013) ("No person, entity, or state agency shall use a manned aircraft, drone or other unmanned aircraft to conduct surveillance . . . of any individual, property owned by an individual, farm, or agricultural industry without the consent of that individual, property owner, farm or agricultural industry"); SB 150, 63d Leg., Reg. Sess. (Mont. 2013); H.B. 912, 83d Leg. (Tex. 2013).

17. H.B. 912, 83d Leg. (Tex. 2013) Sec. 423.002 ("A person commits an offense if the person uses or authorizes the use of an unmanned vehicle or aircraft to capture an image without the express consent of the person who owns or lawfully occupies the real property captured in the image."); *see* Jaikumar Vijayan, *Texas Drone Bill Sparks a Battle*, COMPUTERWORLD (May 17, 2013), http://www.computerworld.com/s/article/9239346/Texas_drone_bill_sparks_a_battle_.

18. Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. § 3119f (2013) (criminalizing the use of visual or audio enhancing devices on drones under certain circumstances); Drone Aircraft Privacy and Transparency Act of 2012, H.R. 6676, 112th Cong. (2012) (proposing that civilians submit and be bound by data collection statements enforceable by the FTC).

19. H.R. 637, 113th Cong. § 3119i (2013). This bill explains that states are not preempted from regulating drone flights that occur within the state. This language appears to preempt, whether intentionally or unintentionally, regulation of all drone flights between states. This would be broader preemption than what currently governs aviation law, where state torts have still been held to apply. *See infra* note 16.

II.
FIRST AMENDMENT CONCERNS

Laws governing civilian drone use risk restricting the ability of civilians to engage in legitimate and even essential information gathering. These restrictions will be made in the name of privacy, but they are still restrictions on speech. Courts have not yet determined whether privacy or speech triumphs in this conflict, or more subtly, how privacy and speech interests interact. We are at the beginning of this conversation, not the end of it.[20]

One recent example of behavior that raises these tensions between privacy and the First Amendment is cellphone recording of police activity. States may want to afford citizens protection from being videotaped or audio-recorded without consent, reasoning that such technologically aided recording creates a permanent record that is qualitatively different from note-taking or memory.[21] In fact, there are good arguments that the First Amendment itself requires privacy measures; pervasive surveillance, whether created by private or public actors, has the potential to chill both association and speech.[22] But in recent years, a number of courts have recognized First Amendment protection for videotaping and audio-recording in public.[23] This protection is founded on a right to gather information, as part of speech or a precursor to it.[24]

In a strange twist to this already-complex issue, the police in a number of states have used the wiretap laws that protect citizens from being videotaped without consent to arrest citizens who videotape police activity.[25] Thus, a law that was intended to be privacy protective may in fact prevent oversight over

---

20. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005). *But see* Jane Yakowitz Bambauer, *Is Data Speech?* 66 STAN. L. REV. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231821.

21. *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 10 (2007).

22. *See, e.g.*, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace*, 28 CONN. L. REV. 981 (1996). This argument that privacy in fact often works in service of freedom of expression has also been made from a Fourth Amendment perspective. *See, e.g.*, Priscilla J. Smith, *Much Ado about Mosaics: How Original Principles Apply to Evolving Technology in* United States v. Jones, 14 N.C. J. L. & TECH. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2233561.

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

24. *See* ACLU v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012) *cert. denied*, 133 S. Ct. 651 (2012) ("The act of *making* an audio or audiovisual recording is necessarily included within the First Amendment's guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording. The right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of *making* the recording is wholly unprotected."); *see also Glik*, 655 F.3d at 82 ("As the Supreme Court has observed, 'the First Amendment goes beyond protection of the press and the self-expression of individuals to prohibit government from limiting the stock of information from which members of the public may draw.'").

25. *See* Michael Potere, *Who Will Watch the Watchmen? Citizens Recording Police Conduct*, 106 NW. U. L. REV. 273 (2012); Travis S. Triano, *Who Watches the Watchmen? Big Brother's Use of Wiretap Statutes to Place Civilians in Timeout*, 34 CARDOZO L. REV. 389 (2012).

government functions, thereby empowering law enforcement rather than restricting it.

Courts have split over how they handle these cases. The First Circuit recently found that there is a clearly established First Amendment right to record the police.[26] The Eleventh Circuit has noted that there is a First Amendment "right to record matters of public interest," subject to reasonable time, place, and manner restrictions.[27] The Seventh Circuit considered the Illinois eavesdropping statute, which makes it a felony to audio record a conversation unless all parties to the conversation consent, regardless of whether the communication was private. The Seventh Circuit found that the statute "restricts far more speech than necessary to protect legitimate privacy interests; as applied to the facts alleged here, it likely violates the First Amendment's free-speech and free-press guarantees."[28]

The Third Circuit, by contrast, found that there is no clearly established right to record police officers; the "right to record" is heavily contextual, so it is difficult to determine whether the right exists in a given fact pattern that courts have not yet considered.[29] And notably, even those courts that found a First Amendment right to record have heavily weighed the context of such recordings. Courts have looked to the fact that the subjects were government officials, in public places, or that the action as a whole was a matter of public interest.[30] There are thus substantial unanswered questions about how broad or narrow the First Amendment right to record is, and how broad or narrow privacy measures must be to not impinge on it.

One intuition that frequently arises in privacy cases, both under tort law and under the Fourth Amendment, is that the location of the recording matters. A First Amendment right to record is most likely to outweigh privacy concerns

---

26. Glik v. Cunniffe, 655 F.3d 78, 83 (1st Cir. 2011) (finding that "the First Amendment protects the filming of government officials in public spaces").

27. Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000) (finding that 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").

28. ACLU v. Alvarez, 679 F.3d 583, 586-87 (7th Cir. 2012) *cert. denied*, 133 S. Ct. 651, 184 L. Ed. 2d 459 (U.S. 2012).

29. Kelly v. Borough of Carlisle, 622 F.3d 248, 262 (3d Cir. 2010) ("[W]e conclude there was insufficient case law establishing a right to videotape police officers during a traffic stop to put a reasonably competent officer on 'fair notice' that seizing a camera or arresting an individual for videotaping police during the stop would violate the First Amendment. Although *Smith* and *Robinson* announce a broad right to videotape police, other cases suggest a narrower right. *Gilles* and *Pomykacz* imply that videotaping without an expressive purpose may not be protected, and in *Whiteland Woods* we denied a right to videotape a public meeting.").

30. *See Glik*, 655 F.3d at 83 (finding that "the First Amendment protects the filming of government officials in public spaces"); *City of Cumming*, 212 F.3d at 1333 (finding that 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."); *Alvarez*, 679 F. 3d at 600 ("[T]he eavesdropping statute restricts a medium of expression—the use of a common instrument of communication—and thus an integral step in the speech process. As applied here, it interferes with the gathering and dissemination of information about government officials performing their duties in public.").

in a public space, where one person's privacy collides with other peoples' experience and memory.[31] But creating a special delineation for privacy laws by restricting their application to non-public spaces runs into problems on both ends: public acts sometimes occur in private spaces; and private acts sometimes occur in public spaces.

States might follow this location intuition, and ban drone use over private property. The proposed Missouri drone privacy law, for example, bans video surveillance on any individual's property without consent.[32] So does the proposed Texas Privacy Act.[33] Such laws follow popular intuitions about privacy, because they protect a visual trespass where physical trespass is not allowed. However, they may run into preemption problems, and could also prevent information-gathering essential to political and social movements.[34] In Dallas, for example, a hobbyist drone photographer uncovered pollution by a meat packing plant through aerial observation of activity on the plant's property.[35]

A number of states are currently considering bills sponsored by the cattle industry that criminalize video recording at farms.[36] These bills target activists and journalists who have been recording conditions in industrial agriculture. Whatever one may think of the politics behind food production, it is clear that the video-making is part of an expressive chain of criticism that goes to the heart of the First Amendment. The First Amendment does not prevent people from being arrested for trespass; but if they are legitimately on a property, it might prevent their arrest for recording video of matters of public interest.[37]

U.S. law has long recognized the complicated tension between privacy and accountability.[38] Banning drone photography or videography prioritizes

---

31. *See* Seth Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335 (2011); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 391-92 (1960) (arguing that public photography implicates no privacy right "since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which any one present would be free to see").

32. *See supra* note 16.

33. H.B. 912, 83d Leg. (Tex. 2013).

34. Thanks to John Villasenor for pointing out the possibility of federal preemption of a state ban on drones, and that nonetheless, individual property owners may have the ability to restrict drone flight in the airspace immediately above their property. *See* United States v. Causby, 328 U.S. 256, 264 (1946) ("We have said that the airspace is a public highway. Yet it is obvious that if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere.").

35. Meghan Keneally, *Drone Plane Spots a River of Blood Flowing from the Back of a Dallas Meat Packing Plant*, DAILY MAIL ONLINE (Jan. 24, 2012), http://www.dailymail.co.uk/news/article-2091159/A-drone-splane-spots-river-blood-flowing-Dallas-meat-packing-plant.html.

36. Editorial, *Cattlemen Aiming to Kill Messenger*, S.F. CHRON. (Mar. 22, 2013), http://www.sfgate.com/opinion/editorials/article/Cattlemen-aiming-to-kill-messenger-4377793.php#ixzz2R77DoYUJ.

37. *But see* Food Lion, Inc. v. Capital Cities, 194 F.3d 505, 519 (4th Cir. 1999) (finding that a grocery chain could recover for trespass by reporters who used hidden video cameras while posing as employees).

38. *See* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the*

the privacy rights of photographic subjects over the First Amendment rights of the photographer or videographer. This may be the balance states and courts eventually choose, but as the developing circuit split over videotaping shows, it is not an easy balance to strike.

The important question in privacy regulation of civilian drone use is thus whether this regulation should be enacted by the federal government, or by states. The tension between privacy and First Amendment freedom is unlikely to be resolved in one fell swoop by a federal statute; moreover, federal preemption will preclude state experimentation. Federal legislation is also costlier and more difficult to enact, and risks getting overturned by courts concerned about First Amendment implications. Rather than attempt to get federal legislation right on the first try, and risk having it rejected by First-Amendment-protective courts, we should allow states to run through less costly iterations.

III.
PRIVACY AND FEDERALISM

Civilian drone use is not the first instance where privacy and federalism have crossed paths. In 2006, a broad coalition of companies called for comprehensive federal consumer privacy law that would preempt state legislation.[39] In response, two prominent privacy scholars, Paul M. Schwartz and Patricia C. Bellia, disagreed about the proper balance between federal and state governance of privacy.

On the one hand, Schwartz argued that states can be "important laboratories for innovations in information privacy law."[40] States have been the first to identify significant regulatory areas in privacy law, and have provided innovative approaches to those areas. For example, states were the first to regulate data security breaches, beginning with California's Senate Bill 1386 (S.B. 1386) in 2002.[41] Through diversity, states have offered simultaneous experimentation with different policies. In the data security area, states differ in the standards under which a company must share information about a data security breach.[42]

On the other hand, argued Bellia, state privacy laws often follow federal legislation, pointing to the "importance of federal leadership in information

Common Law Tort, 77 CALIF. L. REV. 957, 996-97, 1010 (1989) ("From the beginning, therefore, the task of the common law has been to balance the importance of maintaining individual information preserves against the public's general interest in information. . . . The ultimate lesson of the tort, then, is the extreme fragility of privacy norms in modern life.").

39. *See* Riva Richmond, *Business Group Calls for Privacy Law*, WALL ST. J., June 21, 2006, at B2.

40. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 916 (2009).

41. *Id.* at 917.

42. *Id.* at 918.

privacy problems."[43] State wiretap statutes, for example, share the federal statutory core while varying across only a few details.

A federal, or mixed state and federal, approach to law enforcement drone use makes perfect sense. A federal law governing law enforcement drone use would follow in the well-trod—albeit, outdated—footsteps of the Electronic Communications Privacy Act (ECPA).[44] Like ECPA, federal legislation on law enforcement drone use could establish a statutory core to be shared by the states, or a statutory floor, permitting state deviation towards more protection. Additionally, because ECPA already establishes a familiar framework for warrants and court orders governing law enforcement surveillance, a federal law enforcement drone statute need not wait on extensive state experimentation. The updates need not be drone-specific, and could cover location tracking, video surveillance, or use of biometric identification, or other new technologies, if these are the concerns raised by drone surveillance.

As noted, legislation governing video or photographic surveillance by civilian drone users will be far trickier. It will have to navigate the Scylla and Charybdis of privacy and the First Amendment. And if enacted federally, it will deviate from how privacy regulation has historically been divided between the federal government and the states.

There is no federal omnibus privacy law in the United States. Federal privacy law consists of a series of sectoral regulations, enacted somewhat haphazardly. One federal statute governs privacy in video watching, one governs drivers' license information, one governs health information, one governs financial privacy, and so on.[45] Drone-specific regulation would add to this patchwork.

State privacy torts, by contrast, cover what most people think of when they think of personal privacy and social privacy norms. The four classic privacy torts are the public disclosure of private facts, intrusion upon seclusion, false light, and appropriation.[46] In short, privacy torts govern the way private information is obtained and used. Sometimes, the emphasis is on whether the information is private; and sometimes, the emphasis is on how the information is obtained. State privacy torts thus enforce social notions of personal privacy.

Equally important for this discussion, state privacy laws have, unlike federal laws, been used to govern private video recording and audio recording similar to that contemplated by drone bills. A number of states have all-party consent wiretap laws, including Maryland, New Hampshire, Massachusetts,

---

43. Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L. J. 868, 882 (2009).

44. *See* Stephanie Pell & Christopher Soghoian, *Can You See Me Now: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012).

45. For a list of many of the federal privacy bills, see *Existing Federal Privacy Laws*, CENTER FOR DEMOCRACY AND TECHNOLOGY, https://www.cdt.org/privacy/guide/protect/laws.php (last visited May 13, 2013).

46. *See* Prosser, *supra* note 31.

and Pennsylvania; citizens who audio record parties without consent may be subject to arrest or prosecution. If video recording picks up audio, it is subject to these statutes.

Thus states have been the historical locus of governance of personal privacy, and, as discussed, have also been the locus of recent tensions between privacy and the First Amendment. This makes them the historical site of experimentation with privacy law that collides with the First Amendment.

It is appropriate for state laws to continue to serve that function with respect to civilian drone use. Each state will be able to express privacy values reflective of its own citizens' differing principles and needs, and courts can determine whether these values collide with the First Amendment.

Eventually, state civilian drone laws may converge into a floor that other states can each build on, with the more successful statutes—the ones that survive First Amendment scrutiny in courts— serving as the blueprint for eventual federal legislation. For now, however, we truly do not have a uniform idea of how to balance privacy against speech rights in gathering information. If we federally legislate civilian drone surveillance, we risk creating a Congressional floor that collides with the First Amendment.

IV.
SOME QUALIFICATIONS

This argument is conditioned on several important qualifications. First, Congress must legislatively close the trap door that is the third-party or *Miller* doctrine. The third-party doctrine allows law enforcement to avoid the warrant requirement by getting information from third parties that in turn observe the subject.[47] If courts do not fix this loophole, Congress should require law enforcement to obtain a warrant before obtaining information gathered by private parties that it cannot otherwise obtain without a warrant. Otherwise the flexibility explored by states in regulating private drone use will also turn out to be a way for law enforcement to obtain information gathered by private parties.

Second, state experimentation with private drone surveillance should not preclude federal consideration of broader data privacy regulations, even regulations governing private actors. The aggregation of stored information implicates a different set of both First Amendment and privacy concerns than the initial gathering of individual pieces of information.[48] Thus arguing for state-by-state regulation of information-gathering that implicates First Amendment values does not preclude consideration of federal data privacy protection along the lines of the European Union's Data Protection Directive, which governs the way personal data is processed, moved, and stored.[49]

47. *See* United States v. Miller, 425 U.S. 435 (1976).

48. *See* Richards, *supra* note 20. *But see* Bambauer, *supra* note 20.

49. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) (on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

Third, this Essay does not intend to wrest safety or other basic aviation licensing matters from the Federal Aviation Administration. And the Federal Aviation Administration should use its licensing programs to solve perhaps the biggest puzzle of drone regulation: how to provide notice or at least transparency to those being observed so they can determine whether they have been subjected to a privacy violation. Unlike surveillance by camera phone or most forms of CCTV, drone surveillance will often provide no visible notice to the watched party if the drone is high up in the sky.[50] As Representative Ed Markey proposed in a draft bill, the FAA could, as part of its licensing scheme, require that those using drones for surveillance submit a data collection statement indicating when, where, and for how long such surveillance will take place.[51] The federal government should require such data collection statements to be easily searchable, and aid individuals in obtaining any footage or data gathered about them. Both of these provisions are included in the proposed Markey bill. Alternatively, or in addition to this scheme, the federal government could require drone radio frequency identification ("RFID") "license plates" to track the location of drones at any given time.[52] Tracking drones is essential to establishing whether a tort has occurred in any given state.

Fourth, states should decriminalize the use of basic privacy-protective technologies. It may surprise many to learn that a large number of states have anti-mask laws that criminalize mask-wearing in public, except under certain circumstances.[53] Such laws prevent individuals from choosing to avoid surveillance in public places, inhibiting individuals' expressive choices about whether to remain anonymous.

In a world of increasing surveillance, giving more agency to the watched will justify maintaining protection of the expressive freedom of the watchers.

V.
WHY STATES ARE BETTER

Assuming these conditions are met, Congress should defer to states on privacy regulations governing civilian drone use for video and audio surveillance.[54] States have experience regulating many of the kinds of privacy

---

50. At this time, many drones are very noisy and so provide aural notice. But this feature will change as technology progresses. The proposed military ARGUS drone flies at 20,000 feet and can turn "30 or more square miles into live video sharp enough to spot individual people walking around." *See* Devin Coldewey, *ARGUS Drone Spots You From 20,000 Feet — With Camera-Phone Sensors*, NBC NEWS (Jan. 28, 2013), http://www.nbcnews.com/technology/argus-drone-spots-you-20-000-feet-camera-phone-sensors-1C8149730.

51. Drone Aircraft Privacy and Transparency Act of 2013, H.R. 6676, 112th Cong. (2012).

52. *See* Joseph Lorenzo Hall, *'License Plates' for Drones?* CENTER FOR DEMOCRACY AND TECHNOLOGY (Mar. 8, 2013), https://www.cdt.org/blogs/joseph-lorenzo-hall/0803license-plates-drones.

53. *See* Margot E. Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815 (forthcoming 2013).

54. But again, what we traditionally conceive of as wiretapping is already governed by federal

violations contemplated by those who fear drones, and state legislation permits experimentation with these regulations, subject to crucial feedback from courts on First-Amendment boundaries. Congress should therefore wait to enact regulation of civilian use of drones for information-gathering until more data emerges out of state experimentation. At the least, Congress should avoid preempting state regulation in any drone privacy statute it does enact.

A number of state laws raise questions similar to those likely to be raised by drone regulation. State wiretapping laws, Peeping Tom laws, video voyeurism laws, and paparazzi laws all currently regulate privacy-intrusive photography, videography, and sound recordings.[55]

These laws vary in how they handle the scope of privacy protection against video and photographic intrusion. State wiretap laws, for example, vary in whether they require the consent of one party, or the consent of all parties. They vary in whether there must be a reasonable expectation of privacy in the conversation for a privacy violation to occur, and they vary in whether the act of recording must be surreptitious to be banned.[56]

Peeping Tom statutes criminalize peeping through a hole or other aperture into a person's home. They are sparsely enacted, and relatively ineffective, because they require catching the Tom in the act.[57] Video voyeurism statutes criminalize the viewing, videotaping, or photographing of another without knowledge or consent, when done for the purpose of sexual arousal.[58] Some of these statutes require establishing a reasonable expectation of privacy, and some require that the criminalized image be of a nude or partially nude subject.

Paparazzi statutes ban paparazzi from using special technologies to intrude on the personal life and personal spaces of celebrities.[59] In handling these state statutes, many courts have shown a reluctance to find a reasonable expectation of privacy in public places.[60] However, states could conceivably get around this reluctance if desired, through legislation.

Presumably, states will also try to regulate the taking of photographs, video, or audio recordings from drones, as Texas H.B. 912 currently proposes. Drone anti-surveillance laws thus resemble these state privacy statutes that have led courts to grapple with the appropriate balance between privacy and free speech.

---

law (ECPA), and new federal laws could set a floor for related electronic wiretapping concerns. I argue merely that the application of these laws to video recording and audio recording by private parties implicate different concerns not raised by ECPA and traditionally dealt with by the states.

55. State anti-stalking laws implicate the behavior of videographers and photographers, as well, and are on the books in all fifty states. *See* Villasenor, *supra* note 8, at 505.

56. *See* Triano, *supra* note 25, at 392.

57. *See* Antonietta Vitale, *Video Voyeurism and the Right to Privacy: The Time for Federal Legislation is Now*, 27 SETON HALL LEGIS. J. 381, 390 (2003).

58. *See id.*

59. *See* CAL. CIV. CODE § 1708.8(b) (2011).

60. *See* Nancy Danforth Zeronda, *Street Shootings: Covert Photography and Public Privacy*, 63 VAND. L. REV. 1131, 1138 (2010).

The state wiretap law cases discussed above demonstrate that a wholesale ban on drone-based recordings would implicate a substantial First Amendment interest. A wholesale ban of drone videography would thus likely not be found constitutional, because it would ban an entire medium of expression.[61] But as current state laws demonstrate that a number of narrower privacy protections may be societally acceptable and even necessary, these types of restrictions may be imported into state anti-drone-surveillance legislation.

In the next section, I explore the various ways in which states might legislate to protect privacy implicated by drone use.

VI.
AXES OF DRONE-RELATED PRIVACY LAWS

State regulation of surveillance by civilian-operated drones could vary along a number of axes. I do not mean to suggest a uniform law, or to guarantee that all of these variations would survive First Amendment challenges. But this section attempts to provide states with possible variations for regulation of civilian drone surveillance, based on the axes of existing state privacy laws.

States should avoid banning an entire class of recording technologies. Instead, they might apply reasonable time, place, and manner regulations. For example, a state might decide that certain physical locations should not be subject to drone surveillance, or that such surveillance should be permitted only during certain times. However, as discussed above, states might wish to include exceptions for matters of public interest or actions by public figures, and consider newsworthiness as a defense.[62]

States could alternatively, or in addition, choose to target socially unacceptable behavior on the part of the recorder/drone user, by banning surreptitious use or requiring that drone users obtain consent from recorded parties. But as we have seen with the application of state wiretap laws to cellphone taping of police, focusing on consent alone can result in significant restrictions on First-Amendment-protected activities if all parties being recorded refuse to consent for reasons that have nothing to do with privacy

---

61. ACLU v. Alvarez, 679 F.3d 583, 586-87 (7th Cir. 2012) (observing that the overly broad wiretap statute was unconstitutional because it banned all audio recording, subject to consent of the subjects, and did not consider whether the act of recording was surreptitious, or whether the subjects had a reasonable expectation of privacy in the conversation); *see also* Kreimer, *supra* note 31, at 374 (observing that "captured images . . . fall within the protection of 'freedom of speech'"); Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713, 717 (2000) (observing that banning unlicensed use of film projectors would trigger First Amendment scrutiny not because projectors are speech, but because they are "integral to the forms of interaction that comprise the genre of cinema").

62. For example, Illinois considered updating its eavesdropping law to allow citizens to record audio of police who are on duty and in public. *See, e.g.*, Alissa Groeninger, *Illinois' Outdated Eavesdropping Law Still in Limbo*, CHI. TRIB. (June 24, 2012), http://articles.chicagotribune.com/2012-06-24/news/ct-met-illinois-eavesdropping-law-20120624_1_eavesdropping-law-noland-law-enforcement; *see also* Triano, *supra* note 25, at 422.

restrictions. Instead, just as some state wiretap laws target surreptitious or secret recording, state drone privacy laws could ban surreptitious recording by drones.[63] Under this scheme, if a person is openly recording you, even if they have not obtained your explicit consent, then there would be no privacy violation.

State drone laws could consider the superhuman nature of the technology being used.[64] Some states have banned the use in certain situations of technology that is so enhanced that one has no idea one is being recorded in traditionally private spaces; the California paparazzi statute, for example, penalizes the use and attempted use of a visual or auditory enhancing device that captures "personal or familial activity" that could not otherwise have been accessed without a physical trespass.[65] One proposed federal drone bill models its language after this statute.[66]

States could protect acts from being recorded when the acts themselves are subject to a reasonable expectation of privacy. As mentioned above, a number of courts have recently found that there is no reasonable expectation of privacy in public spaces.[67] Several courts however, have found that there can be a reasonable expectation of privacy in public; the Alabama Supreme Court found that a photograph of a woman's underwear, even though taken in public, was still an invasion of privacy.[68] The California Supreme Court has also recognized that a car crash victim could have an expectation of privacy in her conversations with a nurse and other rescuers, even though the crash took place in public.[69]

States could guide courts by legislatively dictating a reasonable expectation of privacy even in public spaces. The federal Video Voyeurism Prevention Act of 2004 ("VVPA") demonstrates one such effort. The VVPA statutorily defines a reasonable expectation of privacy as including a reasonable

63. *See, e.g.*, MASS. GEN. LAWS ANN. ch. 272 § 99(B)(4) (West 2012) ("The term 'interception' means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication . . . .").

64. *See, e.g.*, Priscilla J. Smith, Nabiha Syed, David Thaw & Albert Wong, *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177 (2011), http://yalelawjournal.org/2011/10/11/smith.html.

65. CAL. CIV. CODE § 1708.8(b) (West 2011).

66. *See* Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. § 3119f (2013) ("It shall be unlawful to intentionally operate a private unmanned aircraft system to capture, in a manner that is highly offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of a [sic] individual engaging in a personal or familial activity under circumstances in which the individual had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.")

67. *See, e.g.*, Nussenzweig v. DiCorcia, No. 108446/05, 2006 WL 304832, at *3-4 (N.Y. Sup. Ct. Feb. 8, 2006) (finding that an Orthodox Hasidic Jewish man photographed in public by a prominent photographer, unbeknownst to him, did not experience an invasion of privacy).

68. Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964).

69. Shulman v. Group W Productions, Inc.. 955 P.2d 469 (Cal. 1998).

person's belief that a private area (genitalia) would not be visible to the public, "regardless of whether that person is in a public or private place."[70] Although the Fourth Amendment does not yet recognize privacy expectations in a public place (although five Justices in *United States v. Jones* indicated that such an expectation exists when surveillance is pervasive), state legislatures may be able to foster a competing recognition through statutes by defining circumstances in which people can have a reasonable expectation of privacy in public.[71]

A series of courts of appeals cases on video surveillance in the mid-1980s through the early 1990s may prove informative. These cases found Fourth Amendment protection from video surveillance of non-public places,[72] and created heightened procedural hurdles for law enforcement use of video surveillance, because such surveillance was hidden, intrusive, indiscriminate, and continuous. State privacy laws address whether surveillance is hidden by asking if recordings were surreptitious, and to some extent assume the intrusiveness of certain technologies (audio recording, photography, videography) compared to others (sketching a picture, for example, or retelling an overheard conversation from memory). But these laws generally fail to ask whether surveillance was indiscriminate—that is, whether it captured more than the potentially newsworthy fact in its scope—and whether the surveillance was continuous. State drone surveillance laws could consider additionally addressing these two axes by penalizing indiscriminate and/or continuous recording, or including those features in a definitional determination that a reasonable expectation of privacy has been violated.

Thus state drone laws could vary according to whether they regulate the time and place of recordings; whether they require consent to record; whether they require surreptitious behavior on the part of the recorder/drone; whether they ban the use of enhancing technologies when recorders peer into traditionally private spaces; whether they require a reasonable expectation of privacy in the recorded act; and whether that reasonable expectation of privacy could be defined to exist within a public space or be implicated by indiscriminate and/or continuous recording.

VII.
DRONE EXCEPTIONALISM

Drones may be the impetus for regulation, but they should not be its end. States should consider enacting general anti-video-surveillance legislation that

70. Video Voyeurism Prevention Act of 2004, 18 U.S.C. §1801(b)(5)(B) (2006).

71. United States v. Jones, 565 U.S. —, 132 S. Ct. 945 (2012) (Sotomayor, J., concurring) (agreeing that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy)*; see also id.* (Alito, J., concurring) (characterizing the question presented as whether the defendant's reasonable expectation of privacy was violated by long-term monitoring of his movements).

72. Freiwald, *supra* note 21, at 10.

is not drone-specific. Drones do differ from existing surveillance technology in important ways, not because of one particular feature but because of an accretion of distinguishing features. But many of these features apply equally to camera phone use, or the use of remote biometric identification by private companies.

Because of their relatively low cost and hovering abilities, drones give rise to a specter of pervasive surveillance, much like existing technology that can be used for surveillance, like camera phones.[73] However, unlike surveillance by camera phone or most forms of CCTV, drone surveillance might provide no visible notice to the watched party.[74] Unlike online surveillance, where, given notice, users at least can decide which sites to visit and which services to employ, drone surveillance gives no agency to the watched party.

Additionally, drone use might not be subject to contextual social privacy norms in the way that, for example, email use is. If you send an email to a friend, you can usually trust that the friend will not forward it (although you cannot trust that your email server won't read it). But you have made no such normatively founded calculation with respect to the use of drones by your neighbors, or neighborhood businesses, or national businesses. With drone surveillance, you have not chosen to send information to a friend you trust; that information is recorded without your assessment that the recorder is a trustworthy party bound to certain privacy norms by her social relationship with you.

Fundamentally drones threaten privacy because of the tools they carry. Drones can engage in a number of kinds of remote surveillance. And many of those tools are addressed, or should be addressed, by sectoral privacy laws. For example, using a drone to intercept conversations by deploying a cell-site simulator should be governed by a law prohibiting wiretapping. Using a drone to track an individual's location should be governed by a law prohibiting location tracking. And using a drone to video somebody should be governed by a law on video surveillance or image capture. Thus, rather than employing a drone-specific solution, state legislators should consider more general updates to laws governing the kinds of surveillance they fear.

The difference between a drone and a camera phone may end up mattering, but this need not result in drone-specific protections. If a drone is in fact more privacy violative than a camera phone, courts could place more weight on privacy violations when considering drone surveillance cases than camera phone cases. This does not, however, mean they should be governed by different statutes.

---

73. *See supra* note 3.

74. Currently, low-cost drones certainly provide audio notice, as they are very noisy. But as this changes, and if private drones are permitted to fly at the level of commercial aircraft, drones may provide no notice at all. *See supra* note 50.

VIII.
PREEMPTION

All discussions of federalism must eventually address the possibility of federal preemption. While this Essay is by no means an exhaustive exploration of this topic, it is worth at least cursorily addressing whether preemption already exists. State privacy regulation of drones does not appear to be currently preempted by federal law, insofar as it does not interfere with how or where flight occurs.[75] One of the proposed federal drone bills, however, does attempt to preempt at least some state regulation.[76]

The location of the drone—that is, whether it flies particularly close to the ground—does not determine who regulates them. Historically, the FAA has regulated (although minimally) low-flying hobbyist aircraft, and now contemplates putting in place more stringent regulations to govern such aircraft when they are used for commercial purposes. Since 1981, the FAA has permitted hobbyists to fly remote-controlled aircraft without FAA licensing, as long as the flight is under 400 feet and within their line of sight.[77] The FAA recently clarified, however, that when such aircraft are used for business purposes, they may require "compliance with applicable FAA regulations and guidance developed for this category." The FAA also plans to host rulemaking specifically directed at drones under 55 pounds.[78] Thus there will be overlap of FAA regulatory authority with state regulation even of small, low-flying drones.

However, FAA regulation of small, low-flying drones does not preclude all state regulation. Congress has not created express statutory preemption of laws governing aerial surveillance, and has even expressly nodded to exceptions to federal preemption in the field of aviation. The original Federal Aviation Act had a savings clause explaining that "[n]othing contained in this Act shall in any way abridge or alter the remedies now existing at common law or by statute."[79] In 1994, Congress amended this clause to explain that a

---

75. *See* Villasenor, *supra* note 8, at 513-514 (noting that while aircraft safety, noise, and operation are governed by the FAA, "the safest legislative role for states with respect to [unmanned aircraft systems] UAS privacy lies in minimizing privacy abuses by non-government UAS operators").

76. Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. § 3119i (2013) ("Nothing in this Act shall be construed to preempt any State law regarding the use of unmanned aircraft systems exclusively within the borders of that State."). This language can be read several ways, but arguably implies preemption of state regulation of drones that fly between states.

77. *See* FAA, ADVISORY CIRCULAR (AC) 91-57, MODEL AIRCRAFT OPERATING STANDARDS (1981)*; see also* FAA, UNMANNED AIRCRAFT OPERATIONS IN THE NATIONAL AIRSPACE SYSTEM 5 (2007), *available at* http://www.faa.gov/about/initiatives/uas/reg/media/frnotice_uas.pdf.

78. *See* FAA Modernization and Reform Act of 2012 § 331(6), H.R. 658, 112th Cong. (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr658enr/pdf/BILLS-112hr658enr.pdf ("The term 'small unmanned aircraft' means an unmanned aircraft weighing less than 55 pounds"); *see id.* § 332(b)(1) (requiring "a final rule on small unmanned aircraft systems that will allow for civil operation of such systems in the national airspace system, to the extent the systems do not meet the requirements for expedited operational authorization under section 333 of this Act").

79. Pub. L. No. 85-726, 72 Stat. 731 (1958) (codified at 49 U.S.C. § 40120(c)).

"remedy under this part is in addition to any other remedies provided by law."[80] Presumably, the 1994 revision still intends to exempt state tort laws, for example, from federal preemption.

A number of courts have found federal preemption of state attempts to impose curfews on airports or enjoin flight patterns over certain areas.[81] But federal aviation law does not preempt state common law tort claims for injuries suffered during crashes.[82] Additionally, federal aviation law does not preempt a city's zoning power on land, because that power does not conflict with air use.[83] However, aviation safety law impliedly preempts state schemes for regulating alcoholic beverages on board an aircraft.[84]

One interesting question will be whether the use of cameras on a drone is considered to fall under the regulatory power of the government in federal airspace, or under the state power to protect its citizens from privacy injuries on land.[85] While to my knowledge there is no extensive system of privacy regulation on airplanes, courts might find that airplane safety regulations impliedly preempt state regulation of cameras on planes, as they did the regulation of alcoholic beverages.

CONCLUSION

In its haste to address the specter of a civilian drone invasion, Congress should not preempt states from enacting privacy laws governing civilian drone use. States have served as laboratories for experimentation in achieving a balance between First Amendment rights and privacy protection. Congress should permit them to continue doing just that, until an appropriate balance is struck and federal regulation of civilian drone use might again be considered.

---

80. 49 U.S.C. §40120(c) (2006).

81. *See* City of Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624, 633 (1973)*; see also* Luedtke v. County of Milwaukee, 521 F.2d 387 (7th Cir. 1975); San Diego Unified Port Dist. v. Gianturco, 651 F.2d 1306 (9th Cir. 1981).

82. Cleveland v. Piper Aircraft, 985 F.2d 1438 (10th Cir. 1993) ("Congress has intended to allow state common law to stand side by side with the system of federal regulations it has developed.").

83. Condor Corp. v. City of St. Paul, 912 F.2d 215 (8th Cir. 1990).

84. U.S. Airways v. O'Donnell, 627 F.3d 1318 (10th Cir. 2010).

85. Another interesting question, raised by John Kincaid in comments on this Essay, is whether local governments in crowded cities might have additional authority to regulate drones at low altitude, owing to city-specific conditions such as wall-to-wall skyscrapers. Local regulation of drone altitude and traffic would have implications for drones' abilities to gather information.