BIBLIOGRAPHY OF CLE READING MATERIALS
JUNE 17, 2015

Data Security and Privacy – Session 2

Austin Choi-Fitzpatrick, *Drones for Good: Technological Innovations, Social Movements, and the State*, J. INT'L AFF., Fall/Winter 2014, at 19.

Edward Humes, *Eyes in the Sky: Will Drones End Privacy as We Know It?*, CAL. LAW., Aug. 2013, at 36.

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

Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed to?* (Ohio St. U. Moritz C. L. Law & Legal Theory Working Paper Series, Paper No. 292, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2592500.

Matthew R. Koerner, Note, *Drones and the Fourth Amendment: Redefining Expectations of Privacy*, 64 DUKE L.J. 1129 (2015).

John Pavolotsky, *Privacy in the Age of Big Data*, 69 BUS. LAW. 217 (2013).

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.

Notes

DRONES AND THE FOURTH AMENDMENT: REDEFINING EXPECTATIONS OF PRIVACY

MATTHEW R. KOERNER†

ABSTRACT

Drones have gained notoriety as a weapon against foreign terrorist targets; yet, they have also recently made headlines as an instrument for domestic surveillance. With their sophisticated capabilities and continuously decreasing costs, it is not surprising that drones have attracted numerous consumers—most notably, law enforcement. Courts will likely soon have to decipher the limits on the government's use of drones under the Fourth Amendment. But it is unclear where, or even whether, drones would fall under the current jurisprudence. Because of their diverse and sophisticated designs and capabilities, drones might be able to maneuver through the Fourth Amendment's doctrinal loopholes.

This Note advocates analyzing drones under an adapted approach to the reasonable-expectation-of-privacy test in Katz v. United States*. Courts should focus more on the test's oft-neglected first prong—whether a person exhibited a subjective expectation of privacy—and analyze what information falls within the scope of that expectation, excluding information knowingly exposed to the plain view of the public. This analysis also considers instances when, although a subjective expectation exists, it may be impossible or implausible to reasonably exhibit that expectation, a dilemma especially relevant to an analysis of drones.*

Courts that adopt the recommended analysis would have a coherent and comprehensible approach to factually dynamic cases

† Duke University School of Law, J.D. expected 2015; Arizona State University, B.S., B.A. 2011. I owe my thanks to the dedicated, adept staff of the *Duke Law Journal* and to Professor Lisa Griffin, who provided me with invaluable guidance and feedback throughout this effort. To my family and friends, thank you for all of your patience and support. And most importantly, I thank my wife Lauren, who has made all of this possible as a source of love and laughter.

challenging the constitutionality of drone surveillance. Until then, the constitutional uncertainties of these cases will likely linger.

INTRODUCTION

Senator Dianne Feinstein, a staunch advocate of governmental surveillance[1] and Chairman of the 113th Congress's Senate Intelligence Committee,[2] recently found herself, rather ironically, as the target of surveillance.[3] One day at her home, Senator Feinstein walked to the window to check on a protest that was taking place outside.[4] Much to her surprise, a small drone[5] hovered on the other side of the window, only inches away, spying on her.[6] The drone immediately flew away.[7]

Senator Feinstein's experience is just one example of drones being used for surveillance within the United States. But her story and others like it[8] have sparked significant controversy over the use of drones for domestic surveillance, which falls within a broader debate

---

1. *See* Spencer Ackerman, *Feinstein Promotes Bill to Strengthen NSA's Hand on Warrantless Searches*, GUARDIAN (Nov. 15, 2013, 10:02 AM), http://www.theguardian.com/world/2013/nov/15/feinstein-bill-nsa-warrantless-searches-surveillance.

2. *Members*, U.S. SENATE SELECT COMM. ON INTELLIGENCE, http://www.intelligence.senate.gov/memberscurrent.html (last visited Sept. 30, 2014).

3. Kathryn A. Wolfe, *Dianne Feinstein Spots Drone Inches from Face*, POLITICO (Jan. 15, 2014, 4:15 PM), http://www.politico.com/story/2014/01/senator-dianne-feinstein-encounter-with-drone-technology-privacy-surveillance-102233.html. This is not the first time that Senator Feinstein has been the subject of surveillance. *See* Mark Mazzetti & Carl Hulse, *Inquiry by C.I.A. Affirms It Spied on Senate Panel*, N.Y. TIMES, Aug. 1, 2014, at A1 ("An internal investigation by the C.I.A. has found that its officers penetrated a computer network used by the Senate Intelligence Committee [chaired by Feinstein and] . . . read the emails of the Senate [staff] . . . .").

4. Wolfe, *supra* note 3. The crowd was supposedly protesting the National Security Agency's spying program. *Id.*

5. The technology often referred to as "drones" is also called Unmanned Aerial Vehicles (UAV), Uninhabited Aerial Systems (UAS), Remotely Piloted Vehicles (RPV), and Remotely Operated Aircrafts (ROA). STEVEN J. ZALOGA, UNMANNED AERIAL VEHICLES: ROBOTIC AIR WARFARE 1917–2007, at 2 (2008). This Note uses "drone" to refer to all of these initialisms and, specifically, for any unmanned, electronic or mechanical instrument that flies and uses sensory technology to acquire information. It uses this term not because of any associated negative connotations but because of public familiarity with the term "drone."

6. Wolfe, *supra* note 3.

7. *Id.*

8. *Cf.* Jason Koebler, *North Dakota Man Sentenced to Jail in Controversial Drone-Arrest Case*, U.S. NEWS & WORLD REP. (Jan. 15, 2014), http://www.usnews.com/news/articles/2014/01/15/north-dakota-man-sentenced-to-jail-in-controversial-drone-arrest-case (reporting on the first person to be arrested and convicted of a crime based on evidence obtained by drone surveillance).

on privacy and governmental surveillance programs.[9] Advocates of robust federal surveillance policies champion governmental surveillance as the only way to prevent terrorist and cyber attacks against the United States.[10] President Barack Obama defended these surveillance programs as "'modest encroachments on privacy'" that "strik[e] the 'right balance' between national security and civil liberties."[11] In comparison, privacy advocates envision these surveillance programs leading to a dystopian, totalitarian government watching over its citizenry—undetected but omnipresent.[12] References to George Orwell's *Nineteen Eighty-Four*[13] abound.[14]

---

9. *See* Andy Pasztor & Jack Nicas, *Drone Plan Draws Privacy Concerns*, WALL ST. J., Nov. 7, 2013, 7:58 PM, http://online.wsj.com/news/articles/SB10001424052702303309504579183711382731676 (reporting that a federal plan to integrate drones into the national airspace "riled critics seeking greater attention to privacy protections" at a time of "heightened public and congressional concern about the government's surveillance capabilities"); *see also* Peter Finn & Ellen Nakashima, *Obama Defends Sweeping Surveillance Standards*, WASH. POST, June 7, 2013, http://www.washingtonpost.com/politics/obama-defends-sweeping-surveillance-efforts/2013/06/07/2002290a-cf88-11e2-9f1a-1a7cdee20287_story.html ("[President Barack] Obama said it was 'healthy for our democracy' to have an open discussion about the balance between privacy and security concerns . . . .").

10. *See* David E. Sanger & Thom Shanker, *N.S.A. Director Firmly Defends Surveillance Efforts*, N.Y. TIMES, Oct. 13, 2013, at A15 (reporting that the Director of the National Security Agency, General Keith Alexander, defended the agency's surveillance programs as the only option to prevent terrorist and cyber attacks against the United States and stated that to do so, the United States must expand these surveillance programs).

11. Justin Sink, *Obama Defends NSA Surveillance Programs as 'Right Balance'*, HILL (June 7, 2013, 6:07 PM), http://thehill.com/video/administration/304165-obama-defends-nsa-programs-as-striking-right-balance. President Obama's statement seems to be the antithesis of Benjamin Franklin's famous warning on trading liberty for safety: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." J.A. LEO LEMAY, 3 THE LIFE OF BENJAMIN FRANKLIN: SOLDIER, SCIENTIST, AND POLITICIAN, 1748–1757, at 474 (2009).

12. *See* Pasztor & Nicas, *supra* note 9 (discussing a bill introduced by U.S. Senator Ed Markey to establish privacy rules governing the use of drones to protect Americans from "'spies in the sky,'" and the passage of drone-privacy laws in eight states during 2013).

13. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). *Nineteen Eighty-Four* has frequently been cited as the poster child for a dystopian, totalitarian government that constantly surveils its citizenry. *See* sources cited *infra* note 14.

14. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 466–67 (1989) (Brennan, J., dissenting) (discussing governmental surveillance and referencing *Nineteen Eighty-Four* by George Orwell); M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 32 (2011) (same); Richard G. Wilkins, *Defining the 'Reasonable Expectation of Privacy': An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1078–79 (1987) (same). In *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court considered a question particularly relevant to drones and their ability to track individuals: whether the government may place a Global Positioning System (GPS) on an individual's vehicle and track her public movements without a warrant. *Id.* at 948. During oral arguments in *Jones*, Orwell's *Nineteen Eighty-Four* was mentioned six times. *See* Transcript of Oral Argument at 13, 25, 27, 33, 35, 57, *Jones*, 132 S. Ct. 945 (No. 10-1259).

Apart from the surrounding privacy-concerns debate, drones currently provide many practical benefits and their projected applications seem limitless.[15] Based on their obvious advantage of being unmanned, drones have the capability to conduct missions previously considered too risky, dangerous, or impracticable. These applications are also provided at continuously decreasing costs and with the latest technological sophistication, such as the capability to see through physical obstructions, to detect various chemical and biological agents in the air, to recognize human faces and license plates, and to fly in strategic, coordinated formations.[16]

As has frequently been the case, however, the benefits of technological advancement come with the risk of abuse and harassment.[17] These risks are greater when the technology is utilized by government entities.[18] This Note examines the challenges that the United States faces in addressing those risks and harmonizing the conflict between government and technology. Has privacy prospered or foundered through the development of technology? More specifically, how will the burgeoning swarm of drones over American soil affect domestic law enforcement, and how will these effects withstand Fourth Amendment[19] scrutiny?

---

15. *See infra* notes 143–49 and accompanying text.

16. *See infra* notes 150–54 and accompanying text, and Part II.B.

17. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 240 (1986) (Powell, J., concurring in part and dissenting in part) (describing the Court's role of "ensur[ing] that Fourth Amendment rights would retain their vitality as technology expanded the Government's capacity to commit unsuspected intrusions into private areas and activities"); *id.* (concluding that the majority opinion's approach "will not protect Fourth Amendment rights, but rather will permit their gradual decay as technology advances"); *see, e.g.*, United States v. Cuevas-Perez, 640 F.3d 272, 276 (7th Cir. 2011) (describing GPS as "a technology surely capable of abuses fit for a dystopian novel"), *vacated and remanded*, 132 S. Ct. 1534 (2012); *see also* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

18. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("[T]he Government's unrestrained power to assemble data . . . is susceptible to abuse."); *see also* Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring) ("Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans . . . .").

19. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

Drones, with their current and projected capabilities, present a perfect storm of issues that fall outside of current Fourth Amendment jurisprudence but still appear to implicate the Fourth Amendment.[20] Drones can maneuver through each and every loophole of the jurisprudence for warrantless searches.[21] They travel on public airways at low or high altitudes, undetected and with little or no undue noise, nuisance, or threat to persons or property.[22] They can utilize sense-enhancing technologies that are, or will soon be, in general public use.[23] And drones can use these technologies to gather an abundance of intimate details and information, previously impossible or impracticable to acquire.[24] Law enforcement is likely to increasingly use drones for domestic surveillance,[25] and this will likely propel drones to the forefront of courts' dockets.[26]

Scholars have written exhaustively on many aspects of the Fourth Amendment, and its intersection with drones has recently

---

20. *See* Scott Bomboy, *A Legal Victory for Drones Warrants a Fourth Amendment Discussion*, NAT'L CONST. CTR. (Feb. 7, 2014), http://blog.constitutioncenter.org/2014/02/a-court-victory-for-drones-warrants-a-fourth-amendment-discussion ("For now, there doesn't seem to be a clear-cut answer [on drone surveillance under the Fourth Amendment] . . . .").

21. This Note addresses exclusively *warrantless* surveillance by drones. It does not advocate a blanket prohibition of the use of drones, their technology, or even a prohibition of their use by law enforcement or public entities. Drones provide numerous advantages in both the private and public setting. Their integration and expansion into the airspace under the FAA Modernization and Reform Act of 2012 (FAA Modernization Act) is greatly needed. For law-enforcement purposes, drones may provide the greatest advancement in decades—minimizing risk to police officers, expanding available information, and reducing policing expenses.

These positive aspects, however, do not negate the virtues of requiring warrants in certain situations. *See Riley*, 134 S. Ct. at 2493 ("[T]he warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" (citation omitted)). Requiring warrants for certain governmental intrusions protects society's privacy expectations and the minimum guarantees of the Fourth Amendment. Furthermore, this system promotes the credibility of law-enforcement surveillance because of the ex ante review of the intrusion by a judge, requiring probable cause before authorizing a warrant.

22. *See infra* Part III.B.

23. *See infra* notes 204–05 and accompanying text.

24. *See infra* note 96 and accompanying text.

25. *See* Koebler, *supra* note 8 (reporting on the first person to be arrested and convicted of a crime based on evidence obtained by drone surveillance).

26. Current events will also likely accelerate the use of drones. *See infra* text accompanying notes 153–58. *But see* Jeff Pegues, *Some Drone Decisions Expected Soon, with Final Rules Likely Years Away*, CBS NEWS (Dec. 29, 2014, 11:26 AM), http://www.cbsnews.com/news/some-drone-decisions-expected-soon-with-final-rules-likely-years-away ("[I]t is nearly certain that the FAA will not meet [the September 2015] deadline. Instead, 2017 seems to be a more realistic time frame.").

received significant attention.[27] Much of the literature on drones and the Fourth Amendment recognizes that it is unclear where—and whether—drones fall within current jurisprudence, and recommends a variety of legislative solutions.[28] But although scholars identify the legal uncertainties with drones, those recommending legislative action endorse a partial solution that only perpetuates the problem that the courts have maintained with respect to technology and the Fourth Amendment. Specifically, just as current Fourth Amendment jurisprudence has failed to keep pace with advancing technology, a legislative approach will also trail behind.[29] This Note addresses these

27. A Westlaw search through law reviews and journals for pieces, published before January 1, 2015, that use the words "drones," "search," and "Fourth Amendment" recovered 250 pieces. Of these, eighty-five were published in 2014; seventy-four were published in 2013; thirty-eight were published in 2012; twelve were published in 2011; and forty-one were published before 2011, the earliest in 1991. For example, see generally Timothy T. Takahashi, *Drones and Privacy*, 14 COLUM. SCI. & TECH. L. REV. 72 (2013); John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL'Y 457 (2013); Philip J. Hiltner, Comment, *The Drones Are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and Its Fourth Amendment Implications*, 3 WAKE FOREST J.L. & POL'Y 397 (2013); Troy Roberts, Comment, *On the Radar: Government Unmanned Aerial Vehicles and Their Effect on Public Privacy Interests from Fourth Amendment Jurisprudence and Legislative Policy Perspectives*, 49 JURIMETRICS J. 491 (2009); Andrew B. Talai, Comment, *Drones and* Jones*: The Fourth Amendment and Police Discretion in the Digital Age*, 102 CALIF. L. REV. 729 (2014).

28. *See, e.g.*, Calo, *supra* note 14, at 29 (arguing that drones may be the "catalyst" to "drag privacy law into the twenty-first century"); Roberts, *supra* note 27, at 516 (arguing that the Fourth Amendment provides few protections against the government's use of drones for surveillance and that legislative and regulatory action is necessary); Villasenor, *supra* note 27, at 508 (arguing for law-enforcement policies and legislation to govern drone usage); *see also* Richard M. Thompson II, CONG. RESEARCH SERV., R42701, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES (Apr. 3, 2013), http://fas.org/sgp/crs/natsec/R42701.pdf; Bart Elias, CONG. RESEARCH SERV., R42718, PILOTLESS DRONES: BACKGROUND AND CONSIDERATIONS FOR CONGRESS REGARDING UNMANNED AIRCRAFT OPERATIONS IN THE NATIONAL AIRSPACE SYSTEM (Sept. 10, 2012), http://fas.org/sgp/crs/natsec/R42718.pdf; *cf.* Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (Alito, J., concurring) ("Legislatures, elected by the people, are in a better position than we are to assess and respond to the [technological] changes that have already occurred and those that almost certainly will take place in the future.").

29. A successful legislative approach to drones, or more broadly to governmental surveillance, is also in many ways unrealistic and unlikely based on the current political context and on Congress's legislative record on Fourth Amendment–like protections. In over 225 years since the Bill of Rights was enacted, many of the significant restrictions on governmental investigations have emerged from the courts, rather than Congress. The Supreme Court has frequently stepped in, or perhaps was forced to step in, to uphold the minimum guarantees against unreasonable searches provided by the Fourth Amendment. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2493 (2014) (holding that the police may not, without a warrant, search through digital information on an arrestee's cell phone); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the police may not, without a warrant, wiretap and listen to a

issues and recommends an adaptive approach to Fourth Amendment jurisprudence in the age of the drone.

For these reasons, it is highly probable that courts will soon confront issues regarding the use of drones for domestic surveillance.[30] This Note argues that when these issues arise, courts should apply the reasonable-expectation-of-privacy test expounded in *Katz v. United States*,[31] and, in doing so, expand on the subjective-expectation-of-privacy requirement. This oft-neglected element of the two-pronged test provides critical analysis that is especially relevant to cases involving drones. In further analyzing and clarifying the subjective-expectation requirement, courts should proceed in three steps. First, they should determine whether the surveilled person "exhibited an actual (subjective) expectation of privacy"—the

---

person's phone call from a public telephone booth); Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that evidence obtained from an unconstitutional search may not be admitted at trial as evidence). The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012), is one rare example of a legislative approach to Fourth Amendment issues.

A legislative solution is unrealistic also because of the current political context. A politician who attempts to support legislative action that would implement a robust protection against governmental surveillance by drones might be attacked as being "soft on crime." *See* BRANDON C. WELSH & DAVID P. FARRINGTON, THE OXFORD HANDBOOK OF CRIME PREVENTION 491 (2012) ("It has often been observed that getting tough with [criminal] offenders carries political benefits."). This political fodder would likely dissuade many politicians, as it has in other contexts in the past, from proposing or voting in favor of a legislative solution similar to those proposed by the sources above. *See* sources cited *supra* note 28. Therefore, a legislative solution is unlikely.

Nonetheless, there are some jurists who have advocated for legislative solutions to remedy complex Fourth Amendment issues. *See, e.g.*, *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring) ("In light of [technological] developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."); Kyllo v. United States, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting) ("It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues [concerning technology] rather than to shackle them with prematurely devised constitutional constraints."). Although these jurists might believe that a legislative solution is preferable, they do not acknowledge that it is likely to occur.

In light of this legislative apathy, it is therefore critical to understand where the Fourth Amendment sets the floor of rights for individuals and what restrictions there are on governmental surveillance by drones.

30. *Cf.* Memorandum Decision and Order Denying Motion to Dismiss at *12, North Dakota v. Brossart, Nos. 32-2011-CR-00049, 00071, 32-2011-CR-00074, 32-2011-CR-00050, 00076, 32-2011-CR-00046, 32-2011-CR-00048, 32-2011-CR-00047 (N.D. Dist. Ct. July 31, 2012), *available at* https://www.nacdl.org/uploadedFiles/files/news_and_the_champion/DDIC/Brossart%20Order.pdf (denying a motion to dismiss or, alternatively, to suppress evidence obtained by a drone because "[t]here was no improper use of a [drone]"); Bomboy, *supra* note 20 (reporting on the first case where a person was arrested and convicted of a crime based on evidence obtained by a drone).

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

threshold issue in order for the Fourth Amendment to apply.[32] Second, if the person held a subjective expectation of privacy, courts should evaluate the scope of that privacy expectation. And third, they should determine whether the person "expose[d] [information] to the 'plain view' of outsiders" and whether the evidence at issue fell within the scope of that exposure.[33]

This Note analyzes drones under current Fourth Amendment jurisprudence and suggests an adapted approach to Fourth Amendment doctrine to help remedy many of the problems presented by drones. Part I discusses Fourth Amendment jurisprudence relevant to an analysis of drone technology. Part II provides an overview of the current market for drones, as well as their current designs and capabilities. Part III analyzes the current doctrinal failings of the relevant Fourth Amendment jurisprudence when applied to drones. Finally, Part IV outlines a more effective analysis of drones under the reasonable-expectation-of-privacy test by analyzing the specific facts that might express a surveilled person's subjective expectation of privacy, the scope of those expressive factors, and whether the information obtained through surveillance was exposed to the plain view of the public. This reemphasized and expanded analysis would likely solve many of the problems presented by the application of current Fourth Amendment jurisprudence to drones.

I. DRONES AND CURRENT FOURTH AMENDMENT JURISPRUDENCE

Under the Fourth Amendment, "[t]he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[34] The Fourth Amendment is the "chief source of privacy protection" in the American justice system.[35] It is intended to empower the government to investigate and enforce laws to a "reasonably satisfactory level," while still restricting these powers.[36] In doing so, it acts as a "bulwark

32. *Id.* at 361 (Harlan, J., concurring).

33. *Id.*

34. U.S. CONST. amend. IV.

35. RONALD JAY ALLEN, WILLIAM J. STUNTZ, JOSEPH L. HOFFMAN, DEBRA A. LIVINGSTON & ANDREW D. LEIBOLD, CRIMINAL PROCEDURE: INVESTIGATION AND RIGHT TO COUNSEL 337 (2011).

36. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 484 (2011).

against police practices that prevail in totalitarian regimes."[37] Fourth Amendment jurisprudence has therefore sought an appropriate balance between the government's investigative and prosecutorial powers and an individual's constitutional rights.

In applying the Fourth Amendment to drones, a court must undertake several relevant inquiries to determine if the government's use of the drone violates the Fourth Amendment. The court must first determine whether a search for Fourth Amendment purposes occurred.[38] If no search transpired, then the Fourth Amendment is not implicated.[39] Second, if a search occurred for which no warrant was issued, the court must consider whether that search was reasonable.[40] Therefore, when analyzing the government's use of drones for domestic surveillance, an issue not yet ruled on by the Supreme Court, the first—and, under current jurisprudence, the most relevant—inquiry is whether this surveillance constitutes a search. This fundamental question plays a significant role in existing Fourth Amendment jurisprudence, and any potentially successful challenge to domestic drone surveillance must first satisfy this inquiry. The issue of whether a search occurred, in addition to whether that search was reasonable, has perplexed courts since the Fourth Amendment's ratification.[41] Fourth Amendment jurisprudence has been heavily criticized by numerous legal scholars and labeled "a mess,"[42] "a theoretical embarrassment,"[43] and "a vast jumble of judicial pronouncements that is not merely complex and contradictory, but often perverse."[44]

---

37. California v. Acevedo, 500 U.S. 565, 586 (1991) (Stevens, J., dissenting).

38. JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES 82 (1999).

39. ALLEN ET AL., *supra* note 35, at 418.

40. DRESSLER & THOMAS, *supra* note 38, at 62, 334.

41. *See* Kerr, *supra* note 36, at 480 ("Fourth Amendment rules can appear to be selected almost at random. The patchwork of results has made search and seizure law a theoretical embarrassment to scholars and judges alike. According to scholars, the law lacks any theoretical grounding. It is cobbled together from 'a series of inconsistent and bizarre results that [the Court] has left entirely undefended.'" (alteration in original) (citation omitted)); *see also* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("[T]he antecedent question whether or not a Fourth Amendment 'search' has occurred is not so simple under our precedent.").

42. Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149 (1998).

43. Kerr, *supra* note 36, at 480.

44. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994).

Through the doctrine's "patchwork of [Fourth Amendment] protections,"[45] two frameworks have arisen for identifying a search: a property-rights paradigm and a privacy-rights paradigm.[46] The traditional property-rights paradigm focuses on common-law property rights and examines the government's conduct under the "trespass," "curtilage," and "open-fields" doctrines. Beginning in the twentieth century, courts also adopted a paradigm that focuses on a person's expectations of privacy and analyzes whether these expectations are both subjectively held and objectively reasonable. These two paradigms recognize the intertwined property and privacy principles inherent in the Fourth Amendment's guarantees from unreasonable searches and seizures.[47]

A. The Property-Rights Paradigm

The property-rights framework uses common-law property rights as the parameters for identifying a search within the meaning of the Fourth Amendment. This approach arose from historical roots in the common law and society's reverence for individual property rights.[48] This paradigm also reflects a simple and transparent doctrinal solution to unreasonable governmental intrusions limited by pre-twentieth century investigatory mechanisms that relied on the natural senses.[49] Such searches typically required a physical trespass to acquire the information sought by the government.[50]

United States v. Jones[51] provides a modern example of the property-rights paradigm under the trespass doctrine. In *Jones*, the Supreme Court considered whether attaching a Global Positioning

45. Kerr, *supra* note 36, at 479.

46. *See* United States v. Jones, 132 S. Ct. 945, 952 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

47. *See* Florida v. Jardines, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring) (describing the connection between property and privacy within the Fourth Amendment).

48. Entick v. Carrington, [1765] 95 Eng. Rep. (K.B.) [817] ("Our law holds the property of every man so sacred that no man can set his foot upon his neighbour's close without his leave. If he does he is a trespasser, though he does no damage at all."). Courts and legal scholars have long considered *Carrington* as "'the true and ultimate expression of constitutional law' with regard to search and seizure" and "'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted." *Jones*, 132 S. Ct. at 949 (quoting Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989)).

49. *See Jardines*, 133 S. Ct. at 1417 ("One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy.").

50. *Jones*, 132 S. Ct. at 950.

51. United States v. Jones, 132 S. Ct. 945 (2012).

System (GPS) to Antoine Jones's vehicle and monitoring his movements on public roads for twenty-eight days without a warrant constituted an unreasonable search.[52] The Court unanimously found that the government's conduct violated the Fourth Amendment, but the justices split over their reasoning for that holding.[53] The majority opinion, written by Justice Antonin Scalia, held that the government's actions violated Jones's Fourth Amendment rights based upon the trespass doctrine.[54] By physically attaching a GPS to Jones's vehicle, the government committed a trespass upon chattel and "encroached on a [constitutionally] protected area," notwithstanding the government's monitoring of the vehicle's movements on public roads.[55] The government's actions therefore constituted an unreasonable search.[56]

Fourth Amendment jurisprudence has extended this property-rights paradigm to the curtilage doctrine. The curtilage of the home is considered as "part of the home itself for Fourth Amendment purposes" and, thus, afforded the same protections.[57] The curtilage consists of the area immediately surrounding a home where the private details of the home naturally extend,[58] and it is "intimately linked to the home, both physically and psychologically."[59] In determining whether an area forms the curtilage, courts have considered a variety of factors, including "the proximity of the area . . . to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put,

52. *Id.* at 948.

53. *Id.* at 947. Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor joined Justice Scalia's opinion holding that the government's conduct constituted a search under the property-rights paradigm. *Id.* at 947, 949. Justice Sotomayor entered a concurring opinion arguing that the government's conduct constituted a search under both the property- and privacy-rights paradigms. *Id.* at 954–55 (Sotomayor, J., concurring). And Justices Ginsburg, Breyer, and Kagan joined Justice Alito's concurring opinion arguing that the government's conduct constituted a search under the privacy-rights paradigm. *Id.* at 964 (Alito, J., concurring).

54. *Id.* at 949.

55. *Id.* at 952.

56. *Id.* at 949.

57. Oliver v. United States, 466 U.S. 170, 180 (1984).

58. *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1414–15 (2013) (finding that the front porch of a home fell within the curtilage); California v. Ciraolo, 476 U.S. 207, 209 (1986) (finding that a "fenced-in backyard" fell within the curtilage). *But see* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (finding that "the open areas of an industrial plant complex . . . spread over an area of 2,000 acres" did not fall within the curtilage).

59. *Ciraolo*, 476 U.S. at 213.

and the steps taken by the resident to protect the area from observation by people passing by."[60] The curtilage is generally easily identifiable and understandable from our common experiences and knowledge.[61] The Supreme Court has found the curtilage to include, among other areas, a front porch to a home[62] and a "fenced-in backyard."[63] The curtilage does not include, however, "the open areas of an industrial plant complex . . . spread over an area of 2,000 acres."[64]

In *Florida v. Jardines*,[65] a 2013 property-rights case, the Supreme Court discussed the Fourth Amendment protections guaranteed to the curtilage as well as the scope of an implicit license to enter the curtilage for certain purposes. Here, the Court considered whether the government's brief physical presence on Joelis Jardines's front porch with a drug-sniffing dog, to investigate if illicit drugs were inside the home, constituted an unreasonable search.[66] The majority held that by entering the curtilage (here, the front porch) and acting beyond an implicit license to approach a home and solicit its occupants (here, using the drug-sniffing dog), the government physically trespassed on a constitutionally protected area and, thus, violated Jardines's Fourth Amendment rights.[67] According to the Court, the type of investigative instrument utilized,[68] the duration of the trespass,[69] and the fact that any law-enforcement officer or citizen could enter the same area to knock on the door and attempt to contact the home's occupants,[70] were all irrelevant.

By contrast, courts have not extended the same guarantees afforded to the home and its curtilage to areas deemed analogous to an open field.[71] Open fields are not required to be either open or fields in the literal sense, but they typically fall outside of the home's

60. United States v. Dunn, 480 U.S. 294, 301 (1987).

61. *Oliver*, 466 U.S. at 182 n.12.

62. *Jardines*, 133 S. Ct. at 1414.

63. *Ciraolo*, 476 U.S. at 209.

64. Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

65. Florida v. Jardines, 133 S. Ct. 1409 (2013).

66. *Id.* at 1413.

67. *Id.* at 1417–18.

68. *Id.* at 1417.

69. *See id.* at 1421 (Alito, J., dissenting) (criticizing the majority opinion for ignoring the short period of time, approximately one or two minutes, during which the events transpired).

70. *Id.* at 1416 (majority opinion).

71. Dow Chem. Co. v. United States, 476 U.S. 227, 235–36 (1986); Oliver v. United States, 466 U.S. 170, 176 (1984).

curtilage.[72] Accordingly, an absence or insufficiency of the enumerated factors establishing the curtilage of a home would denote an open field.[73] The Court has found, for example, that a barn was located in an open field, rather than the curtilage, because the barn was fifty yards from a fence surrounding the home and sixty yards from the home, the barn was not surrounded by a fence, the barn "was not being used for intimate activities of the home," and the resident of the home "did little to protect the barn area from observation by those standing in open fields."[74] Open fields do not share the same setting for private activities and information that the Fourth Amendment protects from governmental intrusions.[75] Thus, a person may not expect privacy in an open field, and the government's conduct generally would not constitute a search.[76]

In *Dow Chemical Co. v. United States*,[77] the Supreme Court considered whether the curtilage or open-fields doctrine applied to the open areas between buildings on a large industrial property.[78] The U.S. Environmental Protection Agency (EPA) conducted warrantless, aerial surveillance of a two-thousand-acre facility owned by Dow Chemical.[79] Finding that the extensive, scattered outdoor areas of the complex were neither precisely the curtilage nor an open field,[80] the Court concluded that the complex was more similar to an open field.[81] Therefore, the Fourth Amendment's guarantees did not extend to these areas, and the government's actions did not constitute a search.[82]

The Supreme Court has recently adapted this property-rights paradigm to investigations of the home that would traditionally fall

72. *Dow*, 476 U.S. at 236, 239 (quoting *Oliver*, 466 U.S. at 180 n.11); *see also, e.g.*, United States v. Dunn, 480 U.S. 294, 304 (1987).

73. *See* California v. Ciraolo, 476 U.S. 207, 221 (1986) (Powell, J., dissenting) (listing the factors relevant to determining whether an area constitutes the curtilage); *Oliver*, 466 U.S. at 171 ("[T]he common law, by implying that only the land immediately surrounding and associated with the home warrants the Fourth Amendment protections that attach to the home, conversely implies that no expectation of privacy legitimately attaches to open fields.").

74. *Dunn*, 480 U.S. at 302–03.

75. *Oliver*, 466 U.S. at 179.

76. *Id.* at 178.

77. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

78. *Id.* at 235.

79. *Id.* at 229.

80. *Id.* at 236.

81. *Id.* at 239.

82. *Id.*

outside the trespass doctrine because they do not complete a traditional, physical trespass. This adaptation, expounded in *Kyllo v. United States*,[83] has extended the property-rights paradigm to certain invasive technologies in order to shelter the Fourth Amendment's guarantees from modern technology.[84] This paradigm will likely play a critical role in evaluating the constitutionality of many sophisticated technologies employed by drones. In *Kyllo*, a federal agent, investigating whether Danny Kyllo was growing marijuana plants using heat lamps inside his home, used a thermal-imaging device from a public roadway to determine if there was an elevated amount of heat emanating from the walls of the home.[85] The Supreme Court considered whether the government's use of the thermal imager constituted an unreasonable search and, more generally, "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy."[86] The majority held that when the government uses sense-enhancing technology to acquire details from within "the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'" then this conduct constitutes an unreasonable search when the technology "is not in general public use."[87]

Although the Court failed to clarify the parameters of general public use, several earlier cases introducing this requirement seemed to require only marginal use or prevalence.[88] For example, in *Florida v. Riley*,[89] the Supreme Court found that helicopter travel was not "unheard of" in the area and that it was not "sufficiently rare" to raise a Fourth Amendment issue.[90] In *Dow*, the Court found a twenty-two-thousand-dollar mapmaking camera to be "conventional."[91] The scope of this general-use element is especially relevant to the impending boom in drone usage and the forthcoming Federal

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

84. *Id.* at 34 (stating that the rule in *Kyllo* "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"); *id.* at 36 ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development.").

85. *Id.* at 29.

86. *Id.* at 34.

87. *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

88. The Court did note, however, that the thermal imager was "relatively crude" and not in general public use. *Id.* at 34, 36.

89. Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion).

90. *Id.* at 450–51.

91. Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

Aviation Administration (FAA) regulations under the FAA Modernization and Reform Act of 2012 (FAA Modernization Act),[92] which will integrate drones into the national airspace.[93]

B. The Privacy-Rights Paradigm

Beginning in the twentieth century, the Supreme Court adopted a new Fourth Amendment doctrine analyzing certain nontrespassory issues under privacy-rights rationales. In recognizing that "the Fourth Amendment protects people, not places," the Court attempted to guide the doctrine's analytical criterion to maintain the Fourth Amendment's guarantees in the face of modern technology.[94] This privacy-rights approach resulted from the Court's recognition of various technological advancements that no longer fell neatly within the property-rights jurisprudence.[95] These new technologies have enabled the government to acquire the same type of information—as well as entirely new types of information—that traditionally could only have been lawfully collected by the government pursuant to a warrant.[96]

The Court first announced the privacy-rights paradigm in *Katz v. United States*. In *Katz*, the government attached a microphone to a public phone booth to listen to and record Charles Katz's telephone conversations.[97] The Court rejected the argument that a Fourth Amendment violation turned on whether a physical trespass had occurred.[98] Instead, it held that the government had violated Katz's reasonable expectation of privacy by listening to his conversation,

---

92. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(a)(3), 126 Stat. 11, 73 (2012).

93. *Id.*

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

95. *See id.* at 353 (holding that the government's conduct violated Katz's privacy rights under the Fourth Amendment and reasoning that "[t]he fact that the electronic device . . . did not happen to penetrate the wall of the booth can have no constitutional significance").

96. *See, e.g.*, Riley v. California, 132 S. Ct. 2473, 2491 (2014) ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form . . . ."); *id.* at 2494–95 ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" (citation omitted)); *id.* at 2496 (Alito, J., concurring) ("Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form.").

97. *Katz*, 389 U.S. at 348.

98. *Id.* at 353.

which was intended to be private once he closed the phone-booth door.[99] The government's actions therefore constituted an unreasonable search.[100] In so holding, the Court reasoned that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[101]

Although the majority opinion diverged from the traditional inquiry regarding property rights as the sole relevant criterion in identifying a Fourth Amendment search,[102] *Katz*'s prominence in Fourth Amendment jurisprudence comes from Justice John Harlan's concurring opinion.[103] Justice Harlan interpreted the majority opinion as holding, in part, that "electronic as well as physical intrusion" into areas where "a person has a constitutionally protected *reasonable expectation of privacy*" can violate the Fourth Amendment, and that "the invasion of a constitutionally protected area by [the government] is . . . presumptively unreasonable in the absence of a search warrant."[104] In finding an invasion of Katz's reasonable expectation of privacy, Justice Harlan established a two-part test for determining whether such an expectation existed.[105] First, a person must "have exhibited an actual (subjective) expectation of privacy."[106] Second, that subjective expectation must "be one that society is prepared to recognize as [objectively] 'reasonable.'"[107]

In the decades following *Katz* and the reasonable-expectation-of-privacy test, the Court confronted the issue of warrantless, aerial surveillance in three key cases.[108] Although each of the cases considered aerial surveillance in some respect, they all added a different dynamic to Fourth Amendment jurisprudence and the

99. *Id.* at 352.

100. *Id.* at 353.

101. *Id.* at 351–52 (citations omitted).

102. *Id.* at 353.

103. The Court subsequently adopted the reasonable-expectation-of-privacy test in *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

104. *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring) (emphasis added).

105. *Id.*

106. *Id.* at 361.

107. *Id.*

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

reasonable-expectation-of-privacy test. And each case informs the approach to drones.

California v. Ciraolo,[109] the first of the aerial-surveillance triad, addressed the constitutionality of warrantless, "naked-eye observation" of the curtilage of a home from above.[110] To investigate an anonymous tip that Ciraolo was growing marijuana in his backyard, police officers flew an airplane over his property, photographing marijuana plants discovered on the property from one-thousand feet above.[111] The Court held that although Ciraolo "manifest[ed] his own subjective intent and desire to maintain privacy" by putting up a fence,[112] his expectation was not one that society was prepared to recognize as reasonable.[113] The majority reasoned that because of the proliferation of air travel, anyone could look down and observe the curtilage of Ciraolo's home with naked-eye observation.[114] The Fourth Amendment does not hold the police to a higher standard and require them "to shield their eyes when passing by a home on public thoroughfares . . . where [they have] a right to be."[115]

Dow, discussed above, also considered the "narrow issue" of whether nontrespassory, aerial surveillance of a large commercial property constituted a Fourth Amendment violation.[116] In *Dow*, the EPA surveilled a two-thousand-acre commercial complex from altitudes of twelve-hundred feet and above.[117] The aircraft used "a conventional, albeit precise, commercial camera commonly used in mapmaking"[118] that cost over twenty-two-thousand dollars in the 1980s and was able to enlarge photographs taken at twelve-hundred feet to identify something as small as a power line about one-half of an inch in diameter.[119] Although the majority opinion focused most of

109. California v. Ciraolo, 476 U.S. 207 (1986).

110. *Id.* at 213.

111. *Id.* at 209.

112. *Id.* at 211. Although it referenced Ciraolo's subjective expectation of privacy, the Court neglected to determine the subjective requirement because the state had waived this issue on appeal. *Id.*

113. *Id.* at 214.

114. *Id.* at 215.

115. *Id.* at 213.

116. Dow Chem. Co. v. United States, 476 U.S. 227, 237 (1986).

117. *Id.* at 229.

118. *Id.* at 238.

119. *Id.* at 242 n.4, 243 (Powell, J., concurring in part and dissenting in part).

its analysis on the open-fields doctrine[120] and the facts of *Ciraolo*, which had been decided on the same day as *Dow*,[121] it also cited the reduced expectations of privacy in commercial properties and the type of technology utilized by the government as relevant to its inquiry.[122] The Court reasoned that because expectations of privacy in commercial properties are lesser than those in a home, the Fourth Amendment does not extend to commercial properties as it does to the home.[123] The majority opinion also suggested that the use of "highly sophisticated surveillance equipment not generally available to the public" might constitute an unreasonable search.[124] The technology used by the EPA, however, was not so sophisticated and revealing as to constitute an unreasonable search.[125]

The third and final case, *Florida v. Riley*,[126] was decided three years after *Ciraolo* and *Dow* and garnered only a plurality vote of the Court.[127] In *Florida v. Riley*, the Supreme Court considered whether warrantless, naked-eye aerial observation of the interior of a partially enclosed greenhouse violated the Fourth Amendment.[128] Police officers, investigating an anonymous tip, flew a helicopter four-hundred feet over Riley's greenhouse, which was located ten to twenty feet from his home.[129] Because sections of the greenhouse roof were missing, the officers were able to see inside the greenhouse and identify marijuana plants through naked-eye observation.[130]

Although finding that the greenhouse was within the curtilage, the Court held that the government's conduct did not constitute a search for Fourth Amendment purposes.[131] The plurality opinion reasoned that because the interior of the greenhouse was visible from above through the missing roof panels, Riley could not reasonably expect this area to be free from lawful observations from the public

120. *Id.* at 234–39 (majority opinion).

121. Both cases were decided on May 19, 1986, and Chief Justice Warren Burger authored both majority opinions. California v. Ciraolo, 476 U.S. 207, 207 (1986); *Dow*, 476 U.S. at 227.

122. *Dow*, 476 U.S. at 237–39.

123. *Id.* at 237–38 (quoting Donovan v. Dewey, 452 U.S. 594, 598–99 (1981)).

124. *Id.* at 238.

125. *Id.*

126. Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion).

127. *Id.* at 445–47.

128. *Id.* at 447–48.

129. *Id.* at 448.

130. *Id.*

131. *Id.* at 450, 452.

airspace.[132] Moreover, the Court emphasized that the government's actions did not violate any laws or regulations and that there was no indication that similar helicopter flights were sufficiently rare in the United States to support a reasonable expectation of privacy from this type of observation.[133]

II. THE CURRENT STATE OF DRONE TECHNOLOGY

Although drones have received more public attention recently, they have already played a significant role in both U.S. and world history. Recent events—and federal legislation—indicate that this trend is likely to continue. The current market for drones is at an all-time high, and public and private demand for drones continues to grow.[134] Continuing development of sophisticated drone technology, in addition to decreasing costs, will further increase this demand.[135]

A. The Current Market for Drone Technology

Earlier prototypes of drones were much different than those in the news today, and the use of drones has expanded since their creation.[136] A predecessor to the drone first appeared in American military history during the American Civil War, when both Union and Rebel forces deployed balloons filled with explosive devices against each other.[137] During World War I, the U.S. Navy tested and developed "aerial torpedoes," a form of remote-controlled, explosive drones that would be flown into targets, including "German U-boats, their bases, and munitions factories[,] from distances of up to 100 miles."[138] Although these aerial torpedoes were not sufficiently accurate to be used during World War I,[139] they were eventually flown in World War II.[140] And during the Vietnam War, the U.S. military used drones for surveillance, intelligence gathering, "leaflet

132. *Id.* at 450.

133. *Id.* at 451–52.

134. *See infra* notes 154–55 and accompanying text.

135. *See infra* Part II.B; notes 150–53 and accompanying text.

136. *See generally* LAURENCE R. NEWCOME, UNMANNED AVIATION: A BRIEF HISTORY OF UNMANNED AERIAL VEHICLES (2004); ZALOGA, *supra* note 5.

137. Jim Garamone, *From U.S. Civil War to Afghanistan: A Short History of UAVs*, U.S. DEP'T OF DEFENSE (Apr. 16, 2002), http://www.defense.gov/news/newsarticle.aspx?id=44164. These exploding balloons were supposedly not "terribly effective." *Id.*

138. NEWCOME, *supra* note 136, at 18.

139. ZALOGA, *supra* note 5, at 6.

140. Garamone, *supra* note 137.

dropping," and "radar detection, location[,] and identification" of surface-to-air missiles.[141] Drones are now frequently used to surveil and to conduct air strikes on terrorists and terrorist organizations.[142]

Today, drones have evolved from their militaristic roots and are used for a variety of purposes.[143] As of 2014, drones have been used to monitor weather patterns,[144] to assist in farming and ranching,[145] to patrol international borders,[146] to map and photograph remote locations,[147] to conduct search and rescue missions after the 2010 earthquake in Haiti, and to survey damage after the 2011 Fukushima nuclear disaster.[148] And the predicted applications for drones seem limitless. Some drone advocates have projected their use for engineering, firefighting, journalism, preventing animal poaching, and even delivering packages and pizza.[149]

In addition to their sophisticated capabilities and expanding applications, the ever-decreasing cost of drones is further propelling their popularity. Although some drones like the Air Force's RQ-4A/B Global Hawk cost as much as $222.7 million,[150] companies are developing far-less-expensive models—like Apple's Parrot AR.Drone 2.0—that cost as little as a few hundred dollars.[151] In the law-enforcement setting, the retail price for a police helicopter commonly used for ground support or search-and-rescue missions (not including expenses for fuel, maintenance, and manpower) generally exceeds

---

141. *Id.*

142. *See, e.g.*, ZALOGA, *supra* note 5, at 4 (describing a Central Intelligence Agency drone attack on a senior Al Qaeda leader).

143. Daisy Carrington & Jenny Soffel, *15 Ways Drones Will Change Your Life*, CNN (Nov. 18, 2013, 5:23 AM), http://edition.cnn.com/2013/11/03/business/meet-your-friendly-neighborhood-drones.

144. Jason Koebler, *NASA to Use Second Drone to Monitor Hurricanes*, U.S. NEWS & WORLD REP. (May 30, 2013), http://www.usnews.com/news/articles/2013/05/30/nasa-to-use-second-drone-to-monitor-hurricanes.

145. Carrington & Soffel, *supra* note 143.

146. William Booth, *More Predator Drones Fly U.S.-Mexico Border*, WASH. POST, Dec. 21, 2011, http://www.washingtonpost.com/world/more-predator-drones-fly-us-mexico-border/2011/12/01/gIQANSZz8O_story.html.

147. Jason Koebler, *Drones Could be Coming to American Skies Sooner Than You Think*, POLITICO MAG. (Jan. 28, 2014), http://www.politico.com/magazine/story/2014/01/drones-faa-lawsuit-coming-to-american-skies-102754.html#.UvbYJXk2_wI.

148. Jonathan Beale, *Drones: A Rare Glimpse at Sophisticated US Spy Plane*, BBC NEWS (Oct. 30, 2013, 8:37 PM), http://www.bbc.co.uk/news/world-us-canada-24729998.

149. Koebler, *supra* note 147.

150. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-294SP, DEFENSE ACQUISITIONS: ASSESSMENTS OF SELECTED WEAPON PROGRAMS 113 (2013).

151. Thompson, CONG. RESEARCH SERV., *supra* note 28, at 16.

one-million dollars.[152] These high costs have prevented many law-enforcement departments from purchasing helicopters.[153] Drones provide an inexpensive alternative with many of the same—and often greater—capabilities.

In light of these diverse applications, American venture capitalists invested over forty-million dollars in drones during the first nine months of 2013, over twice the total amount in all of 2012,[154] and the total global market for drones was estimated to have hit eighty-nine billion dollars by 2013.[155] Although FAA regulations have somewhat hindered the proliferation of drone usage,[156] this bulwark will soon be removed by pending FAA regulations that will govern federal aviation law. The FAA Modernization Act directs the FAA to develop a plan to safely integrate drones into the national airspace no later than September 30, 2015.[157] The inevitable result of these measures will be a rapid and heavy influx of drone usage in the United States.[158] In fact, the FAA has forecast that nonmilitary persons will operate approximately fifteen-thousand drones by 2020 and thirty-thousand drones by 2030.[159]

These advanced and affordable technologies have attracted many public entities at both the federal and local level. As of November 2013, the FAA had granted 1387 licenses to fly drones, only one of which was issued to a private entity.[160] The U.S. Customs

---

152. Peter Finn, *Privacy Issues Hover Over Police Drone Use*, WASH. POST, Jan. 23, 2011, http://www.washingtonpost.com/national/privacy-issues-hover-over-police-drone-use/2011/01/22/ABEw0uD_story.html.

153. *Id.*

154. Olga Kharif, *As Drones Evolve from Military to Civilian Uses, Venture Capitalists Move In*, WASH. POST, Nov. 1, 2013, http://www.washingtonpost.com/business/as-drones-evolve-from-military-to-civilian-uses-venture-capitalists-move-in/2013/10/31/592ca862-419e-11e3-8b74-d89d714ca4dd_story.html.

155. Carrington & Soffel*, supra* note 143.

156. Kharif, *supra* note 154.

157. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(a)(3), 126 Stat. 11, 73 (2012). *But see* Pegues, *supra* note 26 ("[I]t is nearly certain that the FAA will not meet [the September 2015] deadline. Instead, 2017 seems to be a more realistic time frame.").

158. *See* Koebler, *supra* note 147 (describing the legal limitations on companies selling drones in the United States, and American companies who resort to selling drones abroad in response).

159. FEDERAL AVIATION ADMINISTRATION, FAA AEROSPACE FORECAST: FISCAL YEARS 2010-2030, at 48 (2010), *available at* http://www.faa.gov/data_research/aviation/aerospace_forecasts/2010-2030/media/2010%20Forecast%20Doc.pdf.

160. Koebler, *supra* note 147. The sole private entity was the oil company ConocoPhillips. *Id.* The FAA has also granted six aerial-photography and video-production companies regulatory exemptions, allowing them to fly drones without a license. Press Release, Fed.

and Border Protection (CBP) has flown drones along the U.S.–Mexico border since 2004 to assist its agents.[161] Drones have made their way into the ranks of local law enforcement as well. Several noteworthy law-enforcement departments that have used drone technology include the Houston Police Department, the Miami-Dade Police Department, the Seattle Police Department, and the Federal Bureau of Investigations.[162] According to law-enforcement officials, drones are a "tactical game-changer," and "'[n]ot since the Taser has a technology promised so much for law enforcement.'"[163] One law-enforcement agency, the Georgia Tech Police Department (GTPD), even applied for FAA authorization to fly drones for "special events" and "day-to-day law enforcement operations."[164] Although GTPD's application was ultimately denied, the department planned to deploy drones to the locations of reported situations and emergencies, and the project was "intended . . . [to] provide valuable lessons learned for the use of [drones] for law enforcement nationwide."[165]

B. Current Drone Capabilities

Most of the successes of drones are attributable to their sophisticated technologies and capabilities. Drones are equipped with various technologies for visual surveillance, audio enhancement, and sense-enhancing capabilities, and with sophisticated programming. Drones are manufactured in a variety of sizes, weights, and designs, and with various methods of flight and propulsion. Current models range in size from a wingspan of just three centimeters[166] to over forty meters.[167] Drones range in weight from eighty milligrams[168] to nearly

---

Aviation Admin., U.S. Transportation Secretary Foxx Announces FAA Exemptions for Commercial UAS Movie and TV Production (Sept. 25, 2014).

161. *Unmanned Aerial Vehicles Support Border Security*, CUSTOMS & BORDER PROT. TODAY (U.S. Customs & Border Prot., Washington, D.C.), July–Aug. 2004, *available at* http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

162. *2011–2012 FAA List of Drone License Applicants*, ELEC. FRONTIER FOUND., https://www.eff.org/document/2012-faa-list-drone-applicants (last visited Feb. 8, 2015).

163. Finn, *supra* note 152.

164. *Georgia Tech Police Department Drone Records, Certificate of Authorization*, ELEC. FRONTIER FOUND., https://www.eff.org/document/georgia-tech-police-dept (last visited Feb. 8, 2015).

165. *Id.*

166. Amina Khan, *Meet RoboBee, a Bug-sized, Bio-inspired Flying Robot*, L.A. TIMES (May 2, 2013, 5:11 PM), http://articles.latimes.com/2013/may/02/science/la-sci-sn-flying-robot-robobee-smallest-ever-20130502.

167. *Global Hawk*, NORTHROP GRUMMAN, http://www.northropgrumman.com/capabilities/globalhawk/Pages/default.aspx (last visited Feb. 8, 2015).

seven tons.[169] Although many drones have been designed as traditional fixed- and rotary-wing aircraft, there have been significant developments to the aeronautical design and propulsion of drones enabling them to fly by "flap[ping their] wings," similar to birds and insects.[170]

The SolarEagle and the RoboBee are perhaps two of the best examples that demonstrate the spectrum of advanced drone designs that could be used by law enforcement. The SolarEagle, currently in development by Boeing and the U.S. Defense Advanced Research Projects Agency (DARPA), is projected to have a wingspan of approximately 120 meters and will utilize solar energy as its power source.[171] In comparison, the RoboBee has a wingspan of approximately three centimeters, weighs eighty milligrams, and was inspired by the bee, contributing to its design and propulsion by two insect-like wings that flap 120 times per second.[172] Drones also have reached significant milestones with regard to velocity, altitude, and flight time. Current models are capable of reaching speeds of over 310 knots true airspeed and altitudes of over 60,000 feet.[173] The SolarEagle's use of solar energy is projected to enable it to remain in continuous flight, without recharging or refueling, for over five years.[174]

Drones also employ the most advanced technology available for visual surveillance. One such example is DARPA's Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS).[175] Alleged to be the most sophisticated surveillance technology ever created—and still partially classified—ARGUS can record video footage with 1.8-gigapixel resolution of an area covering fifteen square miles from a drone flying at twenty-thousand feet.[176] The recording automatically tracks all moving objects within the area

168. Khan, *supra* note 166.

169. *Global Hawk*, *supra* note 167.

170. Khan, *supra* note 166.

171. *Boeing Wins DARPA Vulture II Program*, BOEING (Sept. 16, 2010), http://boeing.mediaroom.com/index.php?s=20295&item=1425.

172. Khan, *supra* note 166.

173. *Global Hawk*, *supra* note 167.

174. *Boeing Wins DARPA Vulture II Program*, *supra* note 171.

175. Craig Lloyd, *DARPA Unveils 1.8-Gigapixel Drone Camera, Can Target Hostiles at 20,000 Feet*, SLASHGEAR (Jan. 29, 2013), http://www.slashgear.com/darpa-unveils-1-8-gigapixel-drone-camera-can-target-hostiles-at-20000-feet-29267138.

176. *Id.*

and can magnify objects on the ground as small as six inches.[177] ARGUS can monitor a medium-sized city and record over five-thousand hours of footage per day.[178] Existing drone technology can also recognize and record license plates[179] and faces.[180] Other forms of visual-surveillance technology include the ability to see through obstructions such as clouds, fog, and walls; to identify objects at night;[181] and, possibly, to recognize psychological signals that detect impending violent behaviors.[182]

Drones are able to employ different types of sense-enhancing technology, including audio recorders and "sniffers" that detect biological, chemical, radioactive, and explosive agents in the air.[183] For example, Makel Engineering, Inc. and Pennsylvania State University are currently developing a drone for the U.S. Navy and U.S. Coast Guard that weighs less than one pound and that could be deployed to suspicious vessels to sniff for explosives, chemical and biological weapons, and illicit drugs.[184]

Future drone technology may be even less restricted by the need for human pilots at the controls. Drones can already fly autonomously, or without any human control.[185] Some have expanded on this technology by programming drones to fly in coordinated,

177. *Id.*

178. *Id.*

179. *Cf.* Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, STAR TRIB. (Aug. 17, 2012, 1:13 PM), http://www.startribune.com/local/minneapolis/166494646.html (describing a Minneapolis municipal database that stores data regarding the recent location of personal vehicles based on license-plate photographs taken by high-definition cameras throughout the city).

180. Brian Naylor, *Look, Up in the Sky! It's a Drone, Looking at You*, NPR (Dec. 5, 2011, 12:34 PM), http://www.npr.org/2011/12/05/143144146/drone-technology-finding-its-way-to-american-skies.

181. UNIV. OF WASH. TECH. & PUB. POL'Y CLINIC, DOMESTIC DRONES: TECH. AND POL'Y ISSUES, at 6 (2013), *available at* http://www.law.washington.edu/Clinics/Technology/Reports/DronesLawandPolicy.pdf (last visited Feb. 8, 2015).

182. *Detection and Computational Analysis of Psychological Signals (DCAPS)*, DARPA, http://www.darpa.mil/Our_Work/I2O/Programs/Detection_and_Computational_Analysis_of_Psychological_Signals_(DCAPS).aspx (last visited Feb. 8, 2015).

183. MAKEL ENG'G, INC., COMPACT ELEC. SNIFFER FOR SHIPBOARD LAUNCHED UAV CBRNE DETECTION MISSIONS, at 1, *available at* http://files.meetup.com/1275333/Narcotic%20sniffing%20drone.pdf (last visited Feb. 8, 2015).

184. *Id.*

185. ZALOGA, *supra* note 5; *see also* Audwin Short, *Nano Quadcopter Robots Swarm Video Flying Drones*, YOUTUBE (Feb. 3, 2012), http://www.youtube.com/watch?v=AiCFtmdrvHM (showing multiple drones flying in formation autonomously).

strategic formations with other drones.[186] These coordinated drones can fly in organized columns and rows, in intersecting figure-eight patterns, and through physical obstructions such as windows and doors, along both horizontal and vertical axes.[187]

A critical feature of these designs and capabilities is that these drones may be undetectable to the person or persons observed. Whether it is from thousands of feet away using precise, sense-enhancing technology or mere inches away in an insect-like form, these drones have the capability to conduct surveillance without detection.

Although these current features and prototypes provide tangible—and intriguing—examples of drone technology, they are intended to serve solely as models to analyze under the Fourth Amendment. Importantly, these are only the *current* designs and capabilities of drones, and these models will likely be outdated, possibly even irrelevant, by the time the courts address drone surveillance under the Fourth Amendment.

III. THE DOCTRINAL FAILINGS OF CURRENT FOURTH AMENDMENT JURISPRUDENCE WHEN APPLIED TO DRONES

There are several problems with applying current Fourth Amendment jurisprudence to drones. The factual dynamics of Fourth Amendment cases contribute to the mishmash of Fourth Amendment jurisprudence, and the increased complexity of drone technology will only contribute to the problems with applying either Fourth Amendment search paradigm to drones. First, drones could generally avoid all Fourth Amendment violations under the property-rights paradigm because they can fly on public thoroughfares, thereby avoiding a trespass. Second, although the reasonable-expectation-of-privacy test would provide the most workable test for an analysis of drones, a person would often be unable to satisfy the test's subjective element, and courts have not yet expounded an understandable theory for the objective element. Drones therefore face considerable challenges under the current jurisprudence.

186. Short, *supra* note 185.

187. *Id.*

A. Factual Dynamics of Fourth Amendment Cases

Given its highly context-specific application, a significant feature of the Fourth Amendment is the dynamic factual scenarios that are presented for court review.[188] The government often employs new instruments to investigate and prosecute criminals.[189] Likewise, criminals often employ new instruments to commit crimes and to evade police detection or capture.[190] Ordinary citizens, however, may employ many of these same instruments to accommodate their everyday conveniences and necessities. According to Professor Orin Kerr, this complex dynamic has contributed to the numerous exceptions and seemingly divergent holdings of Fourth Amendment precedent.[191] This dynamic is exacerbated by the diverse designs and capabilities of sophisticated technology—a dynamic that is not alleviated by drone technology.

Law enforcement can strategically use drone technology to avoid current Fourth Amendment prohibitions. The government can navigate the various doctrinal loopholes by altering the designs and capabilities of drones, the location and flight paths of drones, the means of acquiring information, and the types of information acquired. In effect, drones implicate the most factually diverse aspects of an already diverse and unpredictable jurisprudence. Analyzing drones under both the property-rights and privacy-rights paradigms thus presents significant problems for determining when the use of drones constitutes an unreasonable search.

B. Property-Rights Analysis of Drones

Although some narrow instances might raise a Fourth Amendment issue, drones generally would not be hampered under the property-rights paradigm. It is long established that an aircraft traveling over an individual's land does not constitute a trespass.[192] The Supreme Court rejected the common-law concept of *cuius est solum*, *eius est usque ad coelum*—extending a property owner's rights

188. Kerr, *supra* note 36, at 485.

189. *Id.* at 486.

190. *Id.*

191. *See id.* at 487–90 (arguing that judges recognize the factual dynamics and power imbalances resulting from these technologies and attempt to reconcile these dynamics by applying the law in ways to restore the balance of power between the police and society—what Kerr calls the "Equilibrium-Adjustment Theory").

192. United States v. Causby, 328 U.S. 256, 260–61 (1946).

to the center of the earth and the infinite limits of the universe—as a doctrine with "no place in the modern world."[193] In discarding this doctrine, the Court recognized that the "immediate reaches" around property still belong to the owner.[194] These "immediate reaches," however, seem to comprise the literal interpretation of the phrase, as the Supreme Court has concluded that even low-flying aircraft do not enter these reaches. In *Florida v. Riley*, for example, the plurality opinion held that a helicopter flying four-hundred feet over Riley's property did not constitute a trespass in violation of the Fourth Amendment.[195] The plurality opinion did acknowledge, however, that these limits still exist and that not every aerial inspection of a home would survive an inquiry under the Fourth Amendment "simply because the [aircraft] is within the navigable airspace specified by law."[196]

Much of the current use of drones would not constitute a Fourth Amendment violation under the trespass doctrine. Drones are analogous to manned aircraft in many respects because they can fly on the same public thoroughfares abutting private property. The same precedent regarding air travel would therefore control. If that were the case, drones' flight paths—at or above the four-hundred feet in *Florida v. Riley*—would not constitute a trespass for Fourth Amendment purposes. As discussed above, drones have the ability to fly a few inches off the ground and at altitudes of up to sixty-five-thousand feet.[197] Drones flying at lower altitudes could risk a Fourth Amendment violation under the trespass doctrine for being within the immediate reaches of the property. Assuming that they do not fly within these immediate reaches at ground-level altitudes or near taller buildings (for example, outside the window of a high-rise apartment), however, drones would evade trespass violations as other aircraft do. If the government wanted to conduct surveillance, it could also utilize conventional and future methods of surveillance from public areas or from lower levels that would not implicate the trespass doctrine.

The curtilage doctrine also does not provide a significant Fourth Amendment impediment to law enforcement's use of drones. If

193. *Id.*

194. *Id.* at 264.

195. Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality opinion).

196. *Id.*

197. *See supra* text accompanying note 173.

drones fly outside the immediate reaches of property, then they are likely to avoid a trespass within the curtilage. Furthermore, observing details within the curtilage of the home from a lawful location would not constitute an unreasonable search, as government actors are not required "to shield their eyes" from observing the home or its curtilage.[198] A *Jardines*-like scenario might be the exception, but it sets some precedent for the proposition that certain uses of drones to observe the inside of a home constitute a search within the meaning of the Fourth Amendment. If the government entered the curtilage with a drone to obtain information, similar to *Jardines*,[199] then the trespass doctrine would prohibit conduct outside of an express or implied license to enter the curtilage. It is highly improbable, however, that drones would have an express or implied license to enter the curtilage to investigate.

Lastly, the open-fields doctrine provides no greater protection from drones. The Supreme Court has already rejected the idea that the Fourth Amendment applies to open fields.[200] Therefore, the government's use of a drone to obtain information in open fields would not constitute a search for purposes of the Fourth Amendment.

Despite the advanced capabilities and high costs of some drone models, many would fall outside of the Fourth Amendment analysis stated in *Kyllo v. United States*. Most drone usage would not constitute a search under *Kyllo* unless the information is from the *interior* of the home—*Kyllo* did not consider drone surveillance of the home's non-interior areas. This drone surveillance would collect information existing *outside* the home. Therefore, because this information does not exist within the "interior of the home" and presumably would not "otherwise have [required] a physical 'intrusion, into a constitutionally protected area,'"[201] *Kyllo* would not apply to these types of drone surveillance. *Kyllo* would apply, however, to scenarios where a drone uses sense-enhancing technology to obtain information from within the home. In these circumstances, the use of the drone, similar to the thermal imager in *Kyllo*,[202] would

198. California v. Ciraolo, 476 U.S. 207, 213 (1986).

199. *See* Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013) (holding that the presence of a police officer and drug-sniffing dog within the curtilage to investigate for illicit drugs constituted an unreasonable search).

200. Dow Chem. Co. v. United States, 476 U.S. 227, 235–36 (1986).

201. Kyllo v. United States, 533 U.S. 27, 34 (2001).

202. *See id.* at 29–31 (describing the thermal imager used on Kyllo's home).

constitute an unreasonable search by using sophisticated technology not in general public use to obtain information from the home that would have typically required a physical intrusion. For example, using X-ray or infrared technology that is not in general public use to locate persons within a home would violate the *Kyllo* rule and constitute an unreasonable search within the meaning of the Fourth Amendment.

Nonetheless, a dilemma arises when the information is obtained by using an instrument to enhance details available from public areas. For example, consider whether the use of vision-enhancement technology to peer through an open window of a home on a secluded, one-hundred-acre property would fall under *Kyllo*. Here, the information is available from outside the home, but its availability by naked-eye observation is restricted by the vast size of the private property.[203] Acquiring the information is possible, however, from lawful areas (for example, a distant public road) with the vision-enhancement technology. Because the sense-enhancing instrument is necessary to acquire information from within the home and because a physical trespass on the property or inside the home would be necessary without the instrument, a court would confront conduct falling somewhere between the *Kyllo* and *Ciraolo* scenarios.

Furthermore, the Court has not clarified when technology is sufficiently within general public use to avoid a Fourth Amendment violation. The Court's earlier plurality opinion in *Florida v. Riley* that helicopter travel was not sufficiently rare to raise a Fourth Amendment violation[204] indicated that only a marginal level of prevalence might be necessary (given that not many people enjoy the luxuries of helicopter travel). In light of *Florida v. Riley* and *Kyllo*, drones would not yet be in general public use because of the FAA regulations limiting their use almost exclusively to public entities in limited circumstances. With the FAA Modernization Act and the projected expansion of their use,[205] however, drones will likely surpass

203. This scenario is similar to—but distinguishable from—*United States v. Dunn*, 480 U.S. 294 (1987). In *Dunn*, police officers trespassed onto Ronald Dunn's property, passing several fences and gates, and then looked into Dunn's barn from an open field next to it, identifying a laboratory for illicit drugs. *Id.* at 296–99. In the above scenario, if the government were to stand in an open field on the property without a warrant and look through the window, the government's actions would constitute a trespass—but not a search—under *Dunn* and the open-fields doctrine. This scenario, however, presumes that the government does not trespass onto the property and conducts its surveillance from an area where it may lawfully do so.

204. Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality opinion).

205. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(a)(3), 126 Stat. 11, 73 (2012).

the prevalence of helicopters in both the private and public sectors. And many of the technologies employed by drones, such as cameras and audio recorders, are already commonplace. Therefore, drones will likely soon be within general public use under *Kyllo*, and many forms of drone technology would already satisfy the general-use standard.

C. Privacy-Rights Analysis of Drones

With its holding in *Katz*, the Supreme Court adopted a privacy-rights framework for determining whether a search had occurred for Fourth Amendment purposes. In *Katz*, Justice Harlan interpreted the Court's Fourth Amendment jurisprudence as recognizing two key elements for identifying a search.[206] Under this inquiry, a search generally occurs when persons "have exhibited an actual (subjective) expectation of privacy" and when that expectation is "one that society is prepared to recognize as 'reasonable.'"[207]

The Court in *Jones* alluded to the possible Fourth Amendment inquiries that might be implicated in a case involving drone technology. In *Jones*, the Supreme Court suggested that warrantless, nontrespassory surveillance accomplished by traditional means typically would not qualify as an unreasonable search under current Fourth Amendment jurisprudence.[208] The Court conceded, however, that the same surveillance conducted "through electronic means" might constitute "an unconstitutional invasion of privacy."[209] It recognized that courts might have to confront these problems in a "future case where a classic trespassory search is not involved," but declined to address that scenario.[210]

Although the reasonable-expectation-of-privacy test presents the most viable Fourth Amendment doctrine to analyze drones, it has been highly criticized since its inception. The test has been said to "disappoint[] scholars and frustrate[] students for . . . decades."[211] It has frequently been "criti[cized] as circular, . . . subjective and

206. Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring).

207. *Id.*

208. United States v. Jones, 132 S. Ct. 945, 953 (2012).

209. *Id.* at 954.

210. *Id.*

211. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 503 (2007).

unpredictable."[212] Many legal texts forgo explaining the test, instead simply listing the relevant cases and outcomes.[213] With numerous contrary holdings and no clear framework to analyze cases, a reasonable expectation of privacy "has largely come to mean what a majority of the Supreme Court Justices" says it means.[214] Courts might, and evidence suggests they do, misidentify what society recognizes as a reasonable expectation of privacy.[215] It has also been criticized as a standard that erodes over time[216] because the development of technology slowly erodes the public's privacy expectations and with it, the reasonable expectation of privacy.[217]

The test's current interpretation and application do not cover many of the different types of surveillance conducted by drones. There are two key problems with applying the reasonable-expectation-of-privacy test to drone surveillance. First, there might not be a practical or reasonable way for persons unaware of their exposure to drones to satisfy the subjective requirement of the test. Second, as described above, the objectively reasonable requirement is highly unpredictable and has resulted in an unclear and unworkable standard.

1. *The Subjective-Expectation-of-Privacy Requirement.* A significant problem with applying the reasonable-expectation-of-privacy test to drones is the subjective requirement of "exhibit[ing] an actual (subjective) expectation of privacy."[218] When the Supreme Court has addressed the subjective requirement, albeit infrequently, it has looked to the presence of various expressive factors. In his concurrence in *Katz*, Justice Harlan stated that the "objects, activities,

---

212. Kyllo v. United States, 533 U.S. 27, 34 (2001) (citations omitted).

213. Kerr, *supra* note 211, at 505.

214. ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS 46 (2003).

215. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 774 (1993) (conducting a survey of 217 participants and comparing the participants' perceptions of whether different law-enforcement investigations are unreasonable with analogous Supreme Court precedent, and concluding that "the Supreme Court's conclusions about the scope of the Fourth Amendment [that is, whether certain governmental conduct is objectively reasonable and therefore does not implicate the Fourth Amendment] are often not in tune with commonly held attitudes about police investigative techniques").

216. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 121 (2002).

217. *Id.* at 139.

218. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

or statements that [a person] exposes to the 'plain view' of outsiders" fail the subjective requirement because the person exhibits no intention of keeping these items private.[219] *Dow* discussed the subjective requirement at length,[220] even though the case was decided primarily under the curtilage and open-fields doctrines.[221] Although the Court disagreed on the probative value of the precautions taken by Dow to protect the privacy of its property, both the majority and the dissent mentioned several measures that might indicate a party's subjective expectation of privacy, including a perimeter fence, security personnel, and other precautions against intrusion.[222] The Court in *Ciraolo* also considered a fence around Ciraolo's property as relevant to the subjective inquiry but concluded that the fence did not establish whether he manifested a subjective expectation of privacy from *all* types of observation.[223]

Now consider drones with the capability to conduct surveillance of entire cities, to collect aggregated data on persons that, when taken together, may reveal intimate details, or to collect information believed to be free from unwelcome eyes, ears, and other sensory methods of detection.[224] Each of these methods of surveillance can reveal entirely new types of information, information that is otherwise unattainable without detection, or information that is otherwise prohibitively expensive or difficult to acquire when obtained by traditional surveillance methods. Each makes it impossible or implausible to "*exhibit*[] an actual (subjective) expectation" and intention to keep these details private.[225] And even when it is possible and reasonable to exhibit an expectation of privacy in these scenarios, the Court has failed to expound on what specific

219. *Id.*

220. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 237–38 & n.4 (1986) (discussing the *lack* of precautions taken by Dow to protect the privacy of its property). *But see id.* at 241–43 & nn.1–3, 244 n.7, 247, 249 (Powell, J., dissenting) (discussing the *surplus* of precautions taken by Dow to protect the privacy of its property).

221. *See id.* at 239 (finding that the industrial complex was more similar to an open field than the curtilage).

222. *See id.* at 237 n.4 (discussing precautions taken to protect the privacy of a constitutionally protected area); *id.* at 241–42 (Powell, J., dissenting) (same).

223. California v. Ciraolo, 476 U.S. 207, 211–12 (1986).

224. *See, e.g.*, Finn, *supra* note 152 (discussing the planned deployment of drones to monitor a small town in Afghanistan); Lloyd, *supra* note 175 (discussing ARGUS technology, which can monitor and videotape fifteen square miles and track all moving objects within that area).

225. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (emphasis added).

actions or measures are necessary or sufficient to express a subjective expectation of privacy besides basic precautions, such as perimeter fences and closed phone booths.

There are significant difficulties associated with exhibiting an actual subjective expectation of privacy from several types of drone surveillance. Drones can utilize numerous surveillance methods and can obtain countless types of information. Many people do not expect certain information or details to be at risk of being exposed to others. Consequently, many people will not take typical—or any—precautions to protect the privacy of that information. Although hardly anyone *expects* the government to monitor them and uncover their personal information, this subjective expectation of privacy goes beyond that bare belief that one is not under investigation and extends to the expectation of privacy that people manifest by taking ordinary precautions to protect information from exposure to third parties. This idea extends both to information that people do not expect to be exposed to others by *any* method as well as to information that people do not expect to be exposed because of the precautions they have taken.

Consider, for example, a drone with ARGUS technology, constantly monitoring the location of an individual for a month or longer.[226] Or imagine the insect-like RoboBee conducting dragnet monitoring of a city block and using sniffers to test the air around individuals for specific biochemical agents undetectable by human senses.[227] Current Fourth Amendment jurisprudence regarding the subjective requirement does not inhibit the government from conducting such investigations. A person moving in public "has no reasonable expectation of privacy in his movements from one place to another."[228] Furthermore, a party claiming a violation of his Fourth Amendment rights by these governmental actions would fail the subjective requirement because he has not exhibited his expectation of privacy with respect to this information. Based on the Court's precedent of considering the specific privacy precautions taken, an affected individual would likely fail to take a sufficient precaution,

226. *See, e.g.*, Lloyd, *supra* note 175 (describing ARGUS technology and its surveillance capabilities).

227. *See, e.g.*, Khan, *supra* note 166 (describing the RoboBee); MAKEL ENG'G, INC., *supra* note 183 (describing a drone that sniffs the air for chemical, biological, and narcotic agents).

228. United States v. Knotts, 460 U.S. 276, 281 (1983).

such as concealing his public movements or wearing specific garments to conceal any smells or agents.[229]

Additional problems arise when these measures are impossible or implausible. In *Dow*, the vast property and safety concerns prevented Dow from installing an overhead canopy.[230] Had the Court found the area to constitute the curtilage and not an open field,[231] the lack of a canopy—or a comparable precaution—would have likely negated Dow's expression of a subjective expectation of privacy for the curtilage.[232] It therefore seems that only a dome or structure covering the entire two-thousand-acre property would have been sufficient for the Court to find that Dow exhibited a subjective expectation of privacy in activities occurring within the curtilage of the property.

2. *The Objective-Expectation-of-Privacy Requirement.* There are also significant problems with the reasonable-expectation-of-privacy test's objective requirement that "the [subjective] expectation be one that society is prepared to recognize as 'reasonable.'"[233] Determining whether an expectation of privacy is reasonable turns on "whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[234]

Analyzing whether an expectation of privacy from drone surveillance is objectively reasonable, however, seems to be an informed guess, at best. The Supreme Court has neglected to adopt a single test or approach to determine whether an expectation of privacy is reasonable.[235] The Court has considered many factors in applying the test and has returned a series of "divergent and conflicting" opinions and holdings.[236] This approach has allowed the

229. These scenarios are more likely to turn on the facts of the case, specifically those indicating the extent of the precautions taken and the risk of exposure of the information.

230. Dow Chem. Co. v. United States, 476 U.S. 227, 240 n.1 (1986) (Powell, J., dissenting) ("The record establishes that Dow used the open-air design primarily for reasons of safety . . . . Moreover, . . . Dow found that the cost of enclosing the facility would be prohibitive.").

231. *See id.* at 239 (holding that the area was more analogous to an open field than to the curtilage).

232. *See id.* at 236 ("The intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant.").

233. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

234. Oliver v. United States, 466 U.S. 170, 182–83 (1984).

235. Kerr, *supra* note 211, at 525.

236. Wilkins, *supra* note 14, at 1080.

lower federal courts to justify almost any result.[237] Consequently, an analysis of the reasonableness of drones will depend on their specific use and various intangible factors. Thus, in nearly all Fourth Amendment cases considering governmental surveillance by drones, the objective reasonableness of a subjective expectation of privacy seems up for grabs.

IV. REDEFINING THE REASONABLE-EXPECTATION-OF-PRIVACY TEST

The reasonable-expectation-of-privacy test provides the most viable approach for future cases considering whether the government's use of a drone constitutes an unreasonable search. In applying this test, courts should focus more analysis on the subjective-expectation requirement and expand upon its existing interpretation because this oft-neglected element of the two-pronged test[238] is especially relevant to drones.

In further addressing and clarifying the subjective requirement, the analysis should proceed in three parts. First, a court should determine whether the surveilled person "exhibited an actual (subjective) expectation of privacy"[239] so as to fall within the Fourth Amendment's protections. Second, if the person has exhibited a subjective expectation of privacy, the court should then analyze the scope of that privacy expectation and the information it covers. Finally, the court should determine whether the person has exposed that information to the "'plain view' of outsiders."[240]

A. The Reasonable-Expectation-of-Privacy Test

Adopting a versatile standard focused on the subjective-expectation-of-privacy test may provide the most effective approach to reviewing drone surveillance. This flexible approach accounts for both the diverse factual dynamics of Fourth Amendment cases and

237. *See* Kerr, *supra* note 211, at 525–26 (noting that categorization choices under a policy model can be "completely arbitrary").

238. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 81 U. CHI. L. REV. (forthcoming 2015) (manuscript at 2), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2448617. ("A majority of courts that apply *Katz* do not even mention the subjective test; when the test is mentioned, it is usually not applied; and when it is applied, it makes no apparent difference to case outcomes.").

239. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

240. *Id.*

the nebulous nature of nontrespassory Fourth Amendment issues.[241] It also provides a workable standard for drones and technology in the modern age when the need for Fourth Amendment and privacy protections extends beyond the home and the other traditionally protected areas.[242]

A significant problem with the current interpretation of the reasonable-expectation-of-privacy test is the manner in which the courts have applied the test. Courts have more "flex[ed] than analy[zed]" the test.[243] Moreover, courts have focused almost exclusively on the objective requirement and neglected nearly any analysis of the subjective-expectation requirement.[244] Even when the Supreme Court has addressed the subjective-expectation requirement, it has often failed to clarify what measures are necessary or sufficient to express a subjective expectation of privacy.[245]

Realigning the scope of analysis from the objective requirement to the subjective requirement would solve many of the problems with applying the current interpretation of the reasonable-expectation-of-privacy test to drones. Instead of attempting to analyze and ascertain what expectations of privacy society as a whole would recognize as reasonable, the subjective requirement looks to the specific factual circumstances in determining whether an expectation exists. This realignment would provide a clearer, more consistent analysis for trial courts than the nebulous determinations of the objective requirement.

---

241. *See* Kerr, *supra* note 211 (arguing against a single test or approach for determining the reasonableness of an expectation of privacy because no single test or approach could properly apply to the numerous issues presented by Fourth Amendment cases); *supra* Part I.A. (discussing the factual dynamics of Fourth Amendment cases). *But see* Oliver v. United States, 466 U.S. 170, 181–82 (1984) ("Th[e Supreme] Court repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances. The ad hoc approach not only makes it difficult for the policeman to discern the scope of his authority, it also creates a danger that constitutional rights will be arbitrarily and inequitably enforced." (citations omitted)).

242. Wilkins, *supra* note 14, at 1079.

243. *Id.* (quotation marks omitted).

244. Kerr, *supra* note 238 (manuscript at 2) ("A majority of courts that apply *Katz* do not even mention the subjective test; when the test is mentioned, it is usually not applied; and when it is applied, it makes no apparent difference to case outcomes.").

245. *See supra* text accompanying notes 222–23.

B. The Subjective-Expectation-of-Privacy Requirement

1. *Determining Whether a Subjective Expectation of Privacy Exists*. In determining whether a person holds a subjective expectation of privacy in certain information, various factors might indicate her intention to keep information private. The Supreme Court has detailed some of these factors,[246] but further attention and clarification is needed. Moreover, these expressive factors are not always needed to support a subjective expectation. Fourth Amendment jurisprudence should come to recognize that in certain situations, the lack of evidence exhibiting an expectation of privacy results from the person's belief that the information is at little or no risk of being revealed to others. The lack of expressive factors, therefore, may evidence a robust subjective expectation of privacy that is still entitled to Fourth Amendment protection.

A person can express a subjective expectation of privacy through different expressive factors. These factors "exhibit [an] . . . intention to keep" certain information private.[247] The location of the private information is not determinative or necessary to negate this expectation of privacy. *Katz* described this relationship as follows: "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected."[248]

Although expressive factors provide concrete evidence to ascertain whether a subjective expectation of privacy exists, they may be lacking in cases where the person believes there is little or no risk of having her information revealed to others. In these cases, in which the expectation of privacy is arguably strongest, few people would take measures that would objectively evidence an expectation of privacy. Courts should consider the probability of public exposure and the practicality or reasonableness of taking different information-protecting precautions when determining whether a subjective expectation of privacy exists, even absent previously recognized expressive factors.

For example, consider a RoboBee flying outside the curtilage and immediate reaches of a property and recording a conversation

246. *Id.*

247. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

248. *Id.* at 351–52 (majority opinion) (emphasis added) (citations omitted).

occurring within the curtilage—audible from the public airways overhead but not from the perimeter of the property. Here, most people would not expect the conversation to be exposed to listeners from above. A reasonable individual would believe that a sufficient distance from the perimeter of the property, a normal speaking volume, and an absence of any parties unwelcome to the conversation would be sufficient to indicate that the conversation was intended to be private. The speaker's estimate of a marginal or zero probability of this information being exposed to others demonstrates a subjective expectation of privacy with respect to the information. The lack of expressive factors alone does not fail to create a subjective expectation. Instead, the expectation may be *exhibited* through expressive actions or measures. A subjective expectation of privacy must already exist before it may be exhibited. Expressive factors do not create a subjective expectation; they exhibit it.

Under other circumstances, the impossibility or unreasonableness of taking certain measures to exhibit a subjective expectation of privacy in information also may justify the failure to exhibit any such factors. For example, consider again the hypothetical of a RoboBee using sniffers to test the air around individuals for biological and chemical agents emanating from their persons or effects. If it were known that these investigations actually occurred, people would have little or no opportunity to protect this information and exhibit an expectation of privacy in it. Furthermore, even if some precautions could be taken (for example, wearing a full-body hazmat suit), these precautions would be unreasonable and would impose costly and impractical burdens preventing many individuals from taking such measures. Consequently, people would be subject to these investigations without a feasible way to exhibit their subjective expectation to keep this information private. Imagine if the SolarEagle were used to monitor individuals' locations over an extensive span of time.[249] If a person expects to keep his long-term record of visits to his attorney or psychotherapist private, he would not take burdensome precautions to conceal this information—analogous to a fence around a yard or a closed door of a phone booth—such as repetitively altering the route traveled, the office visited, or his physical and vocal attributes at such meetings.

---

249. *See, e.g.*, Roper, *supra* note 179 (reporting on a "license-plate reader" that digitally recognized and recorded the exact location of the Minneapolis mayor's vehicle at least forty-one times over the course of a year).

These two examples illustrate that the lack of measures exhibiting an expectation of privacy does not negate a subjective expectation of privacy in all circumstances. If it is found that no measures were exhibited, courts determining whether the subjective-expectation requirement was satisfied should first consider the assumed probability of exposure of the information. In addition, they should consider the plausibility and reasonableness of exhibiting a subjective expectation of privacy in that information. Surveilled individuals might still satisfy the subjective requirement by showing either that there was an assumed marginal risk that the information would be exposed or that the only measures available to exhibit a subjective expectation of privacy would have been implausible or impracticable. If a court holds that the person did maintain a subjective expectation of privacy despite the lack of expressive factors, then the scope of that expectation, whether he exposed the information to the plain view of others, and the objective reasonableness of that expectation would still be relevant in determining whether a reasonable expectation of privacy exists to establish a search within the meaning of the Fourth Amendment.

2. *Determining the Scope of the Subjective Expectation of Privacy*. The scope of a person's subjective expectation of privacy is also relevant in determining whether a Fourth Amendment search occurred. Under this inquiry, the scope of the expectation is critical to understanding the extent of the information protected from governmental intrusions. If an expectation of privacy to remain free from intrusion by certain categories of sensory detection extends to only some, but not other, types of information, then any information falling outside of that scope would not be protected. Therefore, the government's acquisition of this unsheltered information would not constitute a search under the Fourth Amendment.

Consider the *Katz* decision itself, in which the Court held that the government's recording of Katz's telephone conversations in an enclosed telephone booth constituted an unreasonable search.[250] By closing the door to the phone booth, Katz exhibited an expectation of privacy for the *oral* content of his phone conversation.[251] The closed door, assuming it was transparent, would not exhibit Katz's expectation of privacy from *visual* observations, including his

250. *Katz*, 389 U.S. at 353.

251. *Id.* at 352.

presence in the phone booth, his use of the telephone, and, possibly, the telephone number he dialed or the contents of the conversation if they were recorded by a lip reader observing the phone booth.[252] Therefore, the scope of Katz's subjective expectation of privacy extended to his oral conversation, but not to these physical characteristics.

3. *Determining Whether a Person Exposed Information to the Plain View of Outsiders*. Justice Harlan expanded on his reasonable-expectation-of-privacy test by clarifying that information "expose[d] to the 'plain view' of outsiders [is] not 'protected'" because no intention to keep it private "has been exhibited."[253] When a person exposes something to the plain view of the public, he also willingly discloses certain information along with it.[254] A voluntary disclosure, however, does not forfeit all related expectations of privacy—or the minimum protections guaranteed by the Fourth Amendment.

Bond v. United States[255] provides a key example of the scope of an exposure of information to others, although the case was decided using the objective-expectation-of-privacy requirement.[256] In *Bond*, a CBP officer checked bus passengers' identifications and squeezed luggage bags in the bus's overhead bins to check for illicit drugs.[257] The officer squeezed Steven Bond's bag and identified a "'brick-like' object," which was found to be a package of methamphetamine.[258] The Supreme Court held that Bond had exhibited a subjective expectation of privacy in the contents of his luggage bag by storing his items within the bag and placing the bag in the overhead bin directly above him.[259] By placing the bag in the public bin, Bond exposed the bag to typical visual observation and casual physical contact by others

252. DRESSLER & THOMAS, *supra* note 38, at 88; *see Katz*, 389 U.S. at 352 ("But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.").

253. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

254. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("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.").

255. Bond v. United States, 529 U.S. 334 (2000).

256. *See id.* at 338–39 (analyzing whether society would recognize Bond's subjective expectation as reasonable and holding that the government's conduct violated his Fourth Amendment rights).

257. *Id.* at 335.

258. *Id.* at 336.

259. *Id.* at 339.

intending to move the bag.[260] The extent of this public exposure, however, did not invite or permit handling of the bag in a purposeful, "exploratory manner."[261]

As *Bond* illustrates, the concept of information "expose[d] to the 'plain view' of outsiders," articulated in Justice Harlan's *Katz* concurrence, relates to the level and extent of the exposure.[262] Just as Bond exposed his bag to only a certain level of observation and handling, a public exposure does not forfeit all expectations of privacy in the protected person or effects. Furthermore, the level of the exposure of information that is readily detectable by others is limited because the information must be exposed to the plain view of the public. People do not expose information to the plain view of the public when acquiring that information would require invasive, sense-enhancing technology or long-term monitoring—surveillance that reveals more information than a plain-view observer is able to uncover.

For example, consider again a RoboBee equipped with a sniffer to test the air for chemical and biological agents. A person probably knows that any strong or detectable odors emanating from his body or effects are susceptible to being smelled by others. The person probably would not believe, however, that scents or agents undetectable by the natural olfactory senses would be at risk of exposure by advanced technology. Not only does he not knowingly or willingly intend to expose this information, but this information is also unavailable to the plain view and the natural senses of the public. The government is able to elicit this information only by inspecting the individual in a purposeful "exploratory manner," similar to the CBP officer squeezing the bag in *Bond*.

Another helpful illustration is the above-mentioned example of an ARGUS-equipped SolarEagle, which monitors an individual for an extended period of time. When the person steps into the public view, he willingly exposes his person and effects to observation by others. The SolarEagle, however, may uncover far more information by compiling an extensive amount of data on the observed person's public activities. By aggregating this information, the SolarEagle could produce a detailed log of every location the person has visited, along with the dates, times, and durations of those visits. This

260. *Id.* at 338.

261. *Id.* at 338–39.

262. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

surveillance reveals more detailed information than what is available to the plain view of the ordinary public observer.

Some might argue that by engaging in any activity, behavior, or expression that is exposed to the public, an individual forfeits all associated expectations of privacy.[263] These opinions fail to recognize that our private lives are not derived solely from the comings and goings that transpire exclusively within the sanctity of the home. Our private lives consist of numerous activities, behaviors, and expressions occurring at home, in public, at work,[264] and in society as a whole—both in solitude and in the presence of others. Secrecy does not equate to privacy and Fourth Amendment jurisprudence must come to reflect this distinction.[265] Although expectations of privacy may be nebulous, individuals still expect certain information to remain private and free from government intrusion. This is the very heart of the Fourth Amendment. And as long established by the Supreme Court, "the Fourth Amendment protects people, not places."[266]

The extent and level of exposure of information to the plain view of the public is especially relevant to drone technology. Just as a "careful [tactile] exploration of the outer surfaces of a person's clothing all over his or her body" violates the sanctity of his body and the level and extent of information he exposes to the public,[267] invasive explorations and investigations of a person or her effects by drones may also violate this sanctity and the extent of the information she has exposed. Thus, by driving an automobile down a public road,

263. *Cf.* Oliver v. United States, 466 U.S. 170, 182 (1984) ("[W]e reject the suggestion that steps taken to protect privacy establish that expectations of privacy in an open field are legitimate."); *Katz*, 389 U.S. at 365 (Black, J., dissenting) (applying a textualist interpretation to a Fourth Amendment issue and concluding that "[a] conversation overheard by eavesdropping, whether by plain snooping or wiretapping, is not tangible and, under the normally accepted meaning of the words, can neither be searched nor seized").

264. In the workplace context, the Supreme Court has "recognized that employees may have a reasonable expectation of privacy against intrusions by police" and "[g]iven the societal expectations of privacy in one's place of work[,] . . . [has] rejected the contention . . . that public employees can never have a reasonable expectation of privacy in their place of work." O'Connor v. Ortega, 480 U.S. 709, 716–17 (1987). This expectation of privacy, however, "must be assessed in the context of the employment relation." *Id.* at 717.

265. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("But whatever the societal expectations [for privacy], [persons] can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite to privacy."); *Oliver*, 466 U.S. at 182 ("The test of [Fourth Amendment] legitimacy is not whether the individual chooses to conceal assertedly '*private*' activity." (emphasis added)).

266. *Katz*, 389 U.S. at 351.

267. Bond v. United States, 529 U.S. 334, 337 (2000) (alteration in original) (quoting Terry v. Ohio, 392 U.S. 1, 16–17 (1968)).

a person exposes the exterior portions of the car to the public, and a law-enforcement officer's observation of the car does not constitute a search.[268] However, many people—including, perhaps, members of the Supreme Court—would find it deeply disturbing for the government to monitor their every move in public.[269] Drones render such monitoring possible. Public movements, however, should not be deemed to expose to the public's plain view an intricate, detailed map of the exact dates, times, and locations of an individual over an extensive period of time. Similarly, individuals should not be deemed to expose the biological and chemical agents emanating from their persons and effects, which may be detected by the hovering RoboBee, to the plain view of the public.

CONCLUSION

When issues concerning the use of drones by the government arise, courts should apply the reasonable-expectation-of-privacy test and expand on the subjective-expectation-of-privacy requirement. In applying the test, they should determine whether there is a subjective expectation of privacy, whether the scope of that privacy expectation extended to the acquired information, and then whether the person exposed the information to the plain view of the public. Analysis of the subjective requirement, however, should not be overlooked as courts have commonly done. Courts should also recognize that an absence of expressive factors exhibiting a subjective expectation of privacy does not defeat a subjective requirement. Expressive factors merely evidence the existence of a subjective expectation; they do not create it. When expressive factors are absent, an individual can still demonstrate that a subjective expectation existed. Finally, courts should also recognize that a subjective expectation of privacy extends to a defined scope of information and that an exposure of this information forfeits the Fourth Amendment protections attached only to the information that is exposed to the plain view of the public.

The analysis outlined in this Note provides guidance for resolving many of the current difficulties in applying Fourth Amendment jurisprudence to drones. These difficulties are especially troubling given the numerous practical benefits that drones could

268. New York v. Class, 475 U.S. 106, 114 (1986).

269. *See* Transcript of Oral Argument at 9–16, *Jones*, 132 S. Ct. 945 (No. 10-1259) (asking whether the government may, without a warrant, monitor the Supreme Court Justices' public movements for a month).

provide to law enforcement and others. The advancement and successes of drone technology, however, will likely be achieved only if there is a proper balance between the government's investigative powers and an individual's constitutional rights, as the Fourth Amendment seeks to achieve. Future cases considering the government's use of drones for surveillance should recognize the critical analysis provided by the subjective requirement. Perhaps only then will Fourth Amendment jurisprudence find an appropriate balance between governmental surveillance by drones and the Fourth Amendment's protections from governmental intrusion.

DRONES FOR GOOD: TECHNOLOGICAL INNOVATIONS, SOCIAL MOVEMENTS, AND THE STATE

Austin Choi-Fitzpatrick

The increased use of and attention to drones, or Unmanned Aerial Vehicles (UAVs), have led to a widespread debate about their application. Much of this debate has centered on their use by governments, often for the purpose of surveillance and warfare. This focus on the state's use obscures the opportunity for civil society actors, including social movements, to make use of these technologies. This article briefly reviews the technological innovation before proceeding to a typology of civil society uses, ranging from art to digital disruption. This typology emphasizes the dual-use nature of this technology and, in the process, highlights the need for a best-practices framework to guide such use. Drone usage for the public good, it is argued, should prioritize 1) subsidiarity; 2) physical and material security; 3) the "do no harm" principle; 4) the public good; and respect for 5) privacy, and 6) data. These factors are introduced and discussed.

The recent wave of mobilization and contestation that has swept from Tunisia to Ukraine has run parallel to the emergence of an important technological innovation.[1] While the use of mobile phones and social media has received a large amount of attention, protests in Hong Kong, Ukraine, and even Ferguson, Missouri have seen the emergence of civil society's use of unmanned aerial vehicles (UAVs) or, more commonly, "drones."[2] This innovation represents a technological shift in scale for citizen journalists, human rights advocates, and social movement actors. As such, it requires a sophisticated assessment of the ethical issues and policy terrain surrounding its use.

To date, debates over the use of UAVs have focused on two areas. First, human rights groups have mobilized against the state's use of drone strikes and the killing of civilians in the "War on Terror." Second, policymakers in Europe and the United States have scrambled to regulate the commercial use of drones. However, a critical third segment of drone usage by and for civil society actors, especially social movements, deserves attention.

Austin Choi-Fitzpatrick is an assistant professor of political sociology at the School of Public Policy at Central European University. Email: choifitza@ceu.hu.

This article reviews the nascent literature on UAV use and situates it within the larger theory and debates over technology and innovation, ethics, legal rights (including privacy and the right to information), public policy, and human rights. It then applies these considerations to proposed guidelines for the use of UAVs by non-state and non-commercial actors.[3] It concludes by noting the perils and promises of the use of drones for the purpose of investigative journalism, human rights monitoring, and state accountability.[4] The dual interest in the technology by both the state and its challengers points to the promise and peril of innovation.

UAVs are an ideal type of innovation, that is, they combine invention with exploitation (by marketing, integrating, and diffusing goods and ideas).

INNOVATION

The promise and peril of UAVs lie at the intersection of three interconnected technological innovations. The first involves a shift from analog to digital devices. This allows for more powerful onboard processors, longer battery life, and the ability to easily stream audio and video to digital consumer devices. Combined with more stable quadcopter designs, these have transferred UAVs from the hobbyist market to the general public. But this shift from analog to digital also covers the payloads these devices carry. While the carrying capacity within consumer devices is modest, they are sufficient to carry cameras, as well as sophisticated signal-jamming equipment, wireless routers, and similar electronic devices. UAVs are an ideal type of innovation, that is, they combine invention with exploitation (by marketing, integrating, and diffusing goods and ideas).[5]

Popular digital imaging devices represent a second technological scale shift, as they generate infinitely portable and reproducible images that can be shared, copied, distributed, and stored with increasing ease and decreasing cost. Combined with the emergence of online environs for storing and sharing images, digital imaging devices have fundamentally disrupted the status quo with regard to journalism, whether for entertainment, such as paparazzi photos of a Hollywood star, or accountability, such as YouTube footage from the Arab Spring.

The third technological innovation, and arguably the most disruptive, is the fundamental break between the camera and the street level. Photography has had a symbiotic connection with the street for more than a century, as far back as Eugène Atget's street photography in Paris in the 1890s and Jacob Riis's documentary photography in New York at the same time.[6] The most memorable photographs of violent conflict, social protest, and natural disaster have almost all been taken by

a person present on the ground. The horizontal plane has been the most important space for both the perambulating human and the observant photojournalist. The same can be said of most state surveillance, as well as the increasingly common use of surveillance cameras in commercial centers. The journalist's camera is positioned at eye level. The state and commercial market have placed their devices just out of arm's reach, but both point nearly horizontally.

UAVs relocate the boundary between what is public and what is private, because camera-equipped UAVs move the line of sight from the street to the air. This simple shift effectively pushes public space from the sidewalk to the stairwell, courtyard, rooftop, and so forth. Once private, these spaces are now subject to surveillance. Or have they now become public spaces? Should technologists, ethicists, and public policy professionals simply increase the number and type of locations that are now considered public, or must a more profound conversation occur?

Technology has redrawn the lines between private and public space. Work on the Internet of Things and Internet privacy suggests that much of what happens in seemingly private spaces is not actually private.[7] This increasingly applies to our browsing habits as well as less recognized data passively generated from devices—for instance, my iPhone's accelerometer telling my mobile carrier or insurance provider that I have not jogged in days. UAVs represent a relatively new technology, or rather, a newly applied technology, that is disrupting our understanding of which spaces are private.

Ubiquitous closed-circuit televisions (CCTVs) represented the vanguard of this change, since they opened sidewalks, parks, and other public spaces to sustained and archived monitoring by commercial interests and law enforcement. When the feed from CCTVs went to tape, the question essentially involved privacy. When the feed now goes to digital archives, subject to hacking and scanning, the privacy issue has grown immeasurably. Digital archives of street surveillance footage, combined with facial recognition and behavioral software, push the privacy issue even further.

While these observations seem pedestrian at first blush, their implications are profound. Security and privacy policies address the prying eyes of the standing observer, not the roving airborne eye of a small UAV that is flying according to Global Positioning System (GPS) waypoints while streaming video over secure Wi-Fi to an operator sitting behind a laptop in a nearby cafe, library, or office complex. "Open air" and "free space" are no longer as "open" or "free" as they once were. They are instead now occupied or vulnerable to occupation. Cyberspace scholars suggest that new technologies are pivotal in "radically restructuring the materiality and spatiality of space."[8] Whether this space is used for the public good or as a means of state and commercial surveillance is just the sort of dilemma

regulators face. Cyber-skeptics fear the panopticon, believing "[a] society biased toward hierarchy and capitalism generates the entirely rational impetus for... surveillance."[9] Others argue for a contrast between libertarian and authoritarian technologies where the former is egalitarian, and the latter is "fundamentally hegemonic."[10] If Predator drone strikes in Pakistan and Yemen represent challenges to notions of sovereignty, camera-equipped civilian UAVs in London and New York represent fundamental challenges to the notion of public space.

For some time, radical geographers have thought about space as it relates to power, politics, and change while technologists focus on the promise and peril of new technology. These two have met in the literature about the Internet.[11] Scholars of online worlds focus on the Internet as a disruptive new space, but UAVs disrupt the actually occurring material and physical space we inhabit every day. This applies to hard security as well as privacy. The walls and barricades around terrorist training camps, Occupy gatherings, and Davos meetings belong to a world of line-of-sight threats from paparazzi and pipe bombs. The United States has reinforced many embassies over the past decade with moats, ramparts, walls, and bulletproof glass.[12] Industry standard protection from an explosives-laden truck, however, is generally useless against a commercially available drone carrying toxic chemicals with an aerosol dispersant flying too close to an air intake inside a military compound. Innovation of this sort is a hallmark of asymmetrical warfare.[13]

Debates between technophiles and techno-skeptics, and the scale shifts indicated above, resonate in a complex thicket of ethical and legal considerations. In the United States, the Federal Aviation Administration (FAA) has attempted to restrict all commercial use of drones, despite questions about their authority to do so.[14] Clearly, UAVs equipped with imaging devices also operate in a cultural, political, and technological environment charged with debates over citizen rights in an age of mobile telephony, citizen journalism, and ubiquitous surveillance. The debates over emerging big data capabilities to harness the data generated by these sources are only now emerging.[15] As societies grapple with the social and ethical implications of these technical innovations, policymakers find themselves in the unenviable position of regulating a technology in its infancy.

CIVIL SOCIETY USES

Like any technology in its early stages of growth, drone use is flourishing. The discussion of the legal terrain surrounding UAVs suggests the challenges posed to the development and implementation of a single policy framework for regulating civilian use. Notably, there are multiple competing analogies for what sort of regulatory puzzle UAVs represent. Are they small airplanes, weapon platforms, flying cameras, or a new hobbyist device? Variation in the answer will shape policy

responses. In what follows, I provide a brief overview of some of the public uses for these devices, the diversity of which suggests the complexity of any policy intervention.

Art

Cinematographers wishing to deploy the technology in the United States have recently petitioned the FAA to allow for their use in commercial artistic production prior to the release of the FAA's decision on drone use in civil airspace. The entertainment industry petition joins three others (agriculture, line inspection, and oil and gas) in seeking a waiver for drone use in "narrowly defined, controlled, low-risk situations."[16] Less conventionally, graffiti artists have begun experimenting with UAVs, the beginning of many efforts to integrate this technology into the arts.[17]

Human rights groups are beginning to make use of space-based remote sensing equipment for monitoring crises, and it is reasonable to expect an increase in such use as prices fall.

Mapping

Mapping represents an important cross-cutting utility that UAVs bring to all of the uses that follow. Maps that are already widely available from commercial enterprises (e.g., Google Maps) can be augmented with UAV-based data on conflicts, disasters, protests, environmental degradation, labor exploitation, and so forth. This usage is not limited to UAV-based equipment, however, as recent innovations include higher quality and lower cost satellite imagery. Human rights groups are beginning to make use of space-based remote sensing equipment for monitoring crises, and it is reasonable to expect an increase in such use as prices fall.[18]

Public Safety

There is increased experimentation with UAVs in a number of public safety-related areas, including firefighting and search-and-rescue operations.[19] UAVs are also deployed to augment the support of traditional ambulance or rescue services, as in the case of an accident in which a small UAV, equipped with a thermal imaging device, was able to locate a wrecked vehicle in Canada, and another in which a camera-equipped drone located a man whom rescue workers had been unable to find for days.[20] Yet such efforts fall into a regulatory gray zone, a fact further complicated by the commercial availability of a weaponized "riot control copter" for use against protesters.[21]

Environment

UAVs are increasingly used in a number of environmental areas, including change mapping (i.e., river erosion, deforestation, and urban expansion); disaster risk management and mitigation (assessing natural disaster risk and monitoring fires, volcanoes, and landslides); monitoring illegal activity, including banned hunting, fishing, and trade; and monitoring other natural factors like migration, levels of endangered species, and foliation.[22] The World Wildlife Fund recently received a $5 million grant from Google's Global Impact Awards program to monitor poaching and the illegal trade in wildlife with UAVs.[23] Large-scale environmental change can also be monitored using UAVs. China is using the technology to monitor polluting industries, and Brazil is considering using drones to monitor illegal logging.[24] Kenya had plans to deploy drones to spy on poachers in fifty-two of its national parks after a pilot program found that their presence reduced poaching by up to 96 percent.[25]

Humanitarian and Development Aid

One of the most significant areas of opportunity for civil society actors is in humanitarian aid, as organizations respond to natural disasters, conflict and post-conflict situations, and more general development and poverty-related needs. Former U.S. ambassador Jack Chow has suggested that UAVs could "deliver a peaceful 'first strike' capacity of food and medicines to disaster areas."[26] UAVs have served just this role in the wake of natural disasters in Haiti and the Philippines.[27] While there is more of a precedent for UAV use in humanitarian and post-conflict settings, they may also prove useful in helping health and development organizations access hard-to-reach beneficiaries.

Journalism

Journalists are increasingly experimenting with the incorporation of drones into their work.[28] Drones allow journalists to get much closer to the action. This applies equally when covering sports, reporting on conflicts, capturing imagery, and generally reporting on stories in ways that had not previously been possible. Citizen journalism could also benefit greatly from the use of UAVs documenting public events and providing alternative avenues for reporting, especially during periods of media censorship.[29]

Corporate Accountability

This use is in its infancy, though it shows promise. Recent drone footage revealed that a meatpacking plant in Texas was illegally dumping pigs' blood from a slaughterhouse into a nearby stream. While this triggered a federal investigation

that shut the plant down, it also led to legislation in Texas forbidding the use of drones over private property.[30] A recent Kickstarter project to monitor factory farms (and challenge so-called "ag-gag" laws passed against whistleblowers and activists) was fully funded in less than a week.[31] It is likely such uses will expand in the near future, especially considering increasing concerns with corporate social responsibility, supply chain ethics, labor rights violations, corruption, and environmental impact.

State Accountability and Conflict

There appears to be a consistent interest in the use of UAVs to monitor low-intensity conflict and peacekeeping.[32] They have recently been deployed by the United Nations (UN) to the Democratic Republic of the Congo, Chad, and the Central African Republic.[33] Rebels in Syria, beyond the definition of civil society advanced here, have deployed relatively affordable and commercially available UAVs to monitor loyalist forces.[34]

A prominent anti-slavery advocate recently suggested deploying drones in the struggle to end slavery and trafficking, in much the same way the technology has been used to protect endangered rhinos.

Human Rights Monitoring

While this usage, like the others listed here, is still in its infancy, it too shows signs of rapid growth. A prominent anti-slavery advocate recently suggested deploying drones in the struggle to end slavery and human trafficking, in much the same way the technology has been used to protect endangered rhinos.[35] In cases such as Syria, there was brief discussion about whether the international community should invoke the Responsibility to Protect doctrine (R2P) and effectively vitiate Syria's rights over its airspace.[36] The Satellite Sentinel Project has advocated a similar intervention in the use of UAVs to monitor crisis situations and human rights violations. In the words of its founders, "A drone would let us count demonstrators, gun barrels, and pools of blood."[37] Sniderman and Hanis argue that, while this approach has implications for sovereignty rights and "may be illegal in the Syrian government's eyes ... supporting Nelson Mandela in South Africa was deemed illegal during the apartheid era."[38] This observation emphasizes the tension between bearing witness and the legal status quo.[39]

Social Movements and Protests

There is some overlap between UAV-based state accountability monitoring and their use in social movements and protests. Clashes between anti-government

protesters and pro-government forces in Bangkok were captured by drones and uploaded to YouTube in an attempt to draw attention to the protestors' cause.[40] They have also been used for similar purposes in Turkey, Estonia, Poland, Hong Kong, and Ferguson, Missouri.[41] This overlap occurs in the area of policing, where social movement scholars and scholars of policing have spent the past decade teasing out the changing dynamics surrounding police–protestor interaction.[42] UAVs can indeed serve as another set of eyes monitoring police action, holding the state to account in potentially violent protests. Yet social movements can put UAVs to a much broader range of uses, the most innovative of which remain to be seen. Whatever the case, civil society actors must be prepared for an aggressive response by the state and its agents, such as when police in Istanbul shot down a camera-equipped UAV while it was monitoring large anti-government protests in the Turkish capital.[43]

Material and Technical Disruption

With art and public safety at one end of the usage spectrum, more disruptive and "hacktivist"-inspired uses lie at the other end. UAVs can be used as lookout posts for graffiti artists or protesters needing a second pair of eyes. Camera-equipped devices can loiter or land and then feed imagery back to a clandestine location. This article has focused on the camera as a particular payload, but UAVs can just as easily carry Wi-Fi hardware that can perform wireless penetration testing, conduct 3D mapping of buildings or urban environments, conduct thermal mapping exercises of indoor and outdoor spaces, and conduct video and audio surveillance through cameras and directional microphones.

This list is meant to be illustrative of broad categories of use, but in reality, there are multiple configurations for a myriad of uses. It is not difficult to devise a modular system that would allow a user to quickly attach just the necessary components and then run multiple passes to update additional layers of data onto a map. For example, a designated area could receive a five-sweep treatment in which the first pass captures video and establishes GPS coordinates, the second captures thermal imagery, the third scans for Wi-Fi data, the fourth scans for radiation levels, and the last captures more specific surveillance footage.[44] The range of uses and the ramifications of various configurations suggest that a sophisticated framework is necessary to guide this innovation.

FRAMEWORKS

This broad and growing list of public uses requires a framework that differs significantly from the guidelines currently being developed around the commercial and military/police use of drones. While these guidelines revolve around security

and profit, the organizing principle for civil society use must emphasize the public good. Current frameworks have broken new ground, but remain sector specific. As seen in Table 1, the Humanitarian UAV Network framework emphasizes safety and suitability with the goal of providing humanitarian support.[45] The Drone Journalism Lab emphasizes transparency and accountability in pursuit of the public good.[46] For its part, the American Civil Liberties Union (ACLU) is focused on privacy, with a focus on preventing police abuse.[47]

Table 1

Existing Guidelines for Drone Usage[48]

Group	Themes	Target	Focal Point (on balance)
ACLU	1. Usage Limits—police use with warrant only 2. Data Retention 3. Policies decided by public representative 4. Abuse Prevention and Accountability 5. Weapons forbidden	Law Enforcement	Restricted Use
Professional Society of Drone Journalists	1. Newsworthiness 2. Safety 3. Sanctity of the law and public spaces 4. Privacy 5. Traditional journalistic ethics	Journalists	Newsworthiness
UAViators.com	*Pre-flight* 1. Do no harm 2. Ensure flight safety (failsafe, flight plan, weather) 3. Ensure humanitarian value 4. Obey all laws 5. Respect individual privacy and engage community 6. Avoid use where retraumatization is possible *In-flight* 1. Select safe sites 2. Use a spotter 3. Respect relevant airspace regulations 4. Use allowed radio-control frequencies *Post-flight* 1. Keep a logbook 2. Request permission for image usage 3. Respect personal privacy and remove identifiable information 4. Freely share imagery with local communities whenever possible	Humanitarian Aid	Harm Reduction

Each contribution listed in the table above advances the factor of the greatest importance to the institutional environment that produced it. A comprehensive framework for civil society drone use must balance many interests: safety, suit-

ability, transparency, accountability, privacy, and the rights of residents (citizen and non-citizen alike), while also maintaining a commitment to the public good. Striking this balance is no easy task. In what follows, I propose a broad framework to guide a range of non-state and non-commercial actor uses of drones. In this light, the guidelines listed above are specific configurations of the broader considerations emphasized in the following six principles:

Subsidiarity – The concept of subsidiarity suggests that decisionmaking and problem solving should occur at the lowest and least sophisticated level possible. The implication here is that a drone should only be used to address situations for which there is not a less sophisticated, invasive, or novel use. Steve Coll, dean of the Journalism School at Columbia University, has argued that drone operators should ask themselves, "What can you use a drone for, that you can't achieve by other means [...]?"[49] Such an approach would ensure that drones are used in areas where they are actually appropriate, thus spurring innovation and possibly reducing resistance to their usage.

Physical and material security – This principle focuses on physical integrity issues related to the use of UAVs. Put bluntly, care must be taken so that these devices do not collide with people or with one another. Furthermore, they must not be weaponized in such a way that could cause physical harm to the public. How exactly this security is ensured is a matter of skill, which is determined by the operator, and situation, which is determined by weather and other environmental conditions. How it is defined is a matter of perspective: It is likely that both governments and corporations will consider the use of UAVs by investigative and citizen journalists to be a violation of their security. This use should nevertheless be protected by the rights to freedom of the press, expression, and information.

Do no harm – This principle draws inspiration from the UAViators' emphasis on a rights-based approach as found in the development and humanitarian aid communities. The focus is not on reducing physical and material security, but is instead on ensuring the public good (i.e., the harm in question is related to the public good rather than physical integrity). The principle is one of proportionality, in which the question to be answered is, "Are the risks of using UAVs in a given humanitarian setting outweighed by the expected benefits?"[50] Here again there is room for debate. It is conceivable that social movements will incorporate UAVs into disruptive tactical repertoires, thereby reducing the likelihood of a policy compromise between movement actors and the centers of power and authority they are challenging. New uses must strike their own balance.

Public interest – This principle draws original inspiration from the concepts of newsworthiness and the public good, while recognizing that some seemingly insignificant or unpopular issues may be in the public's interest and for a public good without being considered newsworthy. This approach is especially sensitive to the importance of investigative journalism that holds to account the powerful and well-resourced, despite attempts by established interests to discredit these efforts.[51] This expansive conceptualization of public accountability is journalism's cornerstone. The preamble to the Society of Professional Journalists' Code of Ethics argues that "public enlightenment is the forerunner of justice and the foundation of democracy."[52] At a time when corporations and the state capture an ever-larger share of private space, every effort must be made to maintain and expand civil society's technological capacity for accountability and resistance. There is no better precedent—as both herald and cautionary tale—for this commitment than the free press.

Citizens and non-citizens should be protected from the prying eyes of the state and commerce, yet there is a need for a larger conversation about what level of privacy is to be expected when civil society actors have deployed drones for their own purposes.

Privacy – Each principle must be held in balance with the others, and none more so than with respect to privacy. Citizens and non-citizens should be protected from the prying eyes of the state and commerce, yet there is a need for a larger conversation about what level of privacy is to be expected when civil society actors have deployed drones for their own purposes.[53] There is reason to believe, however, that current legislation prohibiting "peeking while loitering"—for example, California Penal Code 647(i) prohibits "loitering, prowling, or wandering upon the private property of another, at any time, peeks in the door or window of any inhabited building or structure, without visible or lawful business with the owner or occupant"—would render such spying illegal, regardless of whether the camera was mounted to a tripod or a drone.[54] Yet this framework is more sanguine and ambivalent when it comes to the privacy of powerful rights violators. Camera- or sensor-equipped drones have the ability to violate the privacy and private property rights of corporate persons involved in malfeasance. However, the difference between the privacy of a bedroom and a boardroom is not insignificant. Likewise, creating a framework that applies in all circumstances is nearly impossible in an

era in which digital privacy appears to be a mirage, and the possibility that a new wave of technological innovation will force a fundamental reimagining of both public space and expectations of privacy.

Data protection – Finally, data protection is paramount. Civil society actors using camera-equipped drones are likely to generate sensitive data. Filming a protest event, for example, creates a digital record of protesting participants. In the hands of social movement actors, this footage can be used to mobilize communities or challenge official records of events. In the hands of the authorities, however, digital footage can easily be scanned using facial recognition technology in order to create a database of known activists. As more UAVs gather more data, questions about how to handle big aerial data will emerge. Drones themselves will be easier to hijack as anti-drone technology evolves, and the wireless links that connect them to base stations will also be vulnerable to hacking. Context-specific protocols must ensure the security of data, thereby protecting against physical or digital theft or corruption.

Tensions emerge across these central principles. The first tension lies between individual privacy and the public interest. At the time of writing, it seems clear that privacy is undergoing a substantial overhaul in terms of the level of anonymity that can be reasonably expected in an age of constant surveillance and ubiquitous digitization. While it is difficult to comment on a process that is in flux and is subject to starkly different national regulatory regimes and cultural norms, it is clear that citizens and non-citizens alike will need to accept significantly less-robust guarantees to privacy in the future. This reality brings new tradeoffs, and it is important that those actors using UAVs work within the general bounds of emerging norms about privacy.

The second tension lies between insider and outsider tactics in the use of UAVs. While humanitarian drone use may be integrated into a state's military apparatus, social movements often choose tactics based on their values and goals.[55] Since social movements frequently reject formal political channels, or may be blocked from them altogether, there should be little surprise when they turn to social media in the face of authoritarian oppression.[56] Indeed, this is the recent history of social movements. In Rhodes's vivid description of the New Left in the 1960s, he documents a wide range of tactics:

> Petitioning, rock throwing, canvassing, letter writing, vigils, sit-ins, freedom rides, lobbying, arson, draft resistance, assault, hair growing, nonviolent civil disobedience, operating a free store, rioting, confrontations with cops, consciousness raising, screaming obscenities, singing, hurling shit, marching, raising a clenched fist, bodily assault, tax refusal, guerilla theater, cam-

> paigning, looting, sniping, living theater, rallies, smoking pot, destroying draft records, blowing up ROTC buildings, court trials, murder, immolation, strikes, and writing various manifestoes or platforms.[57]

While a good number of these fail the "do no harm" threshold, their creative breadth in a pre-digital age suggests that any framework for new technology must work hard to strike a balance between freedom of expression and assembly and the security of capital and the state. Policymakers and innovators alike should engage in a broad and inclusive discussion about how these principles might be best balanced.

Talking about these tensions is not easy. Innovation is a moving target.

CONCLUSION

In this article, I have attempted to briefly emphasize a relatively unfamiliar origins story for drones. Commercially available devices challenge the notion that drones are cousins to strike fighters laden with laser-guided bombs; they are also part of the same family as cameras. The technological family metaphors need not stop there. Indeed, the second section of this article is dedicated to detailing ten clear civilian and civil society uses for UAVs. The drone's payload can be beneficial and benign, or disruptive and deadly. My focus here has been on the drone's range of uses. The article's third section provides a tentative framework that I believe will help policymakers and the public differentiate between beneficial and harmful uses, with the "public good" as the benchmark. What exactly constitutes the public good is a matter of debate. Protecting privacy is important, but so is shedding light on important issues and holding responsible parties accountable. Protecting property is important, but so is speaking truth to power through graffiti and protest art.[58]

Talking about these tensions is not easy. Innovation is a moving target. The host of uses described earlier was harvested from online reports of innovation within roughly a twelve-month period. This innovation has occurred despite a lack of sustained scholarly inquiry or stable and consistent governmental oversight. Indeed, it was only recently that the FAA licensed three university campuses to conduct research on drone use.[59] Even without this licensing, others are using money from the U.S. Army Research Laboratory's Army Research Office to incorporate drones into campus-based, Wi-Fi-based mesh network systems.[60] At the risk of severely belaboring the point, innovation has completely outstripped legislation, and much of this innovation is by and for the public good. This will continue into the foreseeable future as additional uses emerge. At present, it is not clear what the relationship will be between "drones for the public good" and satellites gathering

information about humanitarian crises and human rights violations, though organizations such as UAViators are actively integrating social media, aerial imagery, and satellite imagery for humanitarian relief efforts.[61] A broader range of actors is working to make geographic information systems (GIS) and satellite data valuable for advocacy groups and policy practitioners alike.[62] This use predates the current wave of drone use by several years, and it is likely that more effective combinations of these technologies will be developed for civil society use. The Satellite Sentinel Project has the tagline, "The world is watching because you are watching," effectively shifting surveillance from an invasive enterprise to bearing witness.[63] This clever blending of traditional movement concepts (bearing witness) with new means (satellite technology) is echoed by Patrick Meier, who suggests that classic civil resistance tactics can be extended to drones.[64] This can be done, he argues, through the display of flags and symbolic colors, the "haunting" or taunting of officials, nonviolent air raids, defiance of blockades, and the disclosure of the identities of state agents.[65]

An initial wave of enthusiasm will subside, leaving behind a solid body of innovation on the way civil society actors perform a number of tasks, especially related to social movements.

This wave of innovation and welter of uses raises a larger question: Does any of it matter? This is the subsidiarity principle writ large: Is there not another, less dramatic, way to meet these same objectives? What do drones add to the existing citizen monitoring mechanisms, through which information is captured on smartphones and disseminated by social media? These are important questions that I hope ongoing use and subsequent scholarship will begin to clarify. My sense is that an initial wave of enthusiasm will subside, leaving behind a solid body of innovation on the way civil society actors perform a number of tasks, especially related to social movements.

A final complication takes the form of public opinion, which seems hostile to this occupation of airspace. A recent study by the Pew Research Center's Internet & American Life Project found, "Sixty-three percent [of respondents] think it would be a change for the worse if personal and commercial drones are given permission to fly through most U.S. airspace."[66] Likewise, while it is legal in the United States to take pictures of individuals in public places, recent recreational uses have led to complaints of sexual harassment, as well as violence against drone operators.[67] The Kenyan government recently announced that it would ban the use of drones for monitoring poachers in the Ol Pejeta Conservancy, home to the endangered white rhino.[68] South Africa, too, has grounded camera-equipped UAVs,

citing regulatory uncertainty at the global level.[69] Grappling with innovation is no easy task. This article suggests the same can be said of technology's relationship to civil society. Regulators must take care, lest they pass legislation and regulations that enable the state while crippling its citizens. ♚

NOTES

[1] This article benefitted from the research assistantship of M. Boby Sabur, Tautvydas Juskauskas, Luis Cano, and Justin De Los Santos; substantive and technical input from Phil Howard, Patrick Meier, John Holland, Sejal Parmer, Bernhard Knoll-Tudor, Thorsten Benner, Dean Starkman, Colleen Sharkey, Lars Almquist, and Edward Branagan; and financial support from Wolfgang H. Reinicke and the Central European University's School of Public Policy.

[2] This language is fraught. The U.S. military is committed to avoiding the terms "drone" and "unmanned aerial vehicle," preferring instead to use the term "remotely piloted aircraft." This term avoids the implication that these devices fly themselves, as well as the gendered notion that they are flown by men. I prefer the term "remotely piloted aerial platform" to reflect the diversity of payloads and the presence of a pilot, however remote and regardless of gender. I would be pleased if this usage proves popular but will not be using these pages to advance this argument. For present purposes, the common terms "drone" and "UAV" prevail. Jim Garamone, "Military Uses Remotely Piloted Aircraft Ethically," *American Forces Press Service*, 22 May 2014, http://www.defense.gov/news/newsarticle.aspx?id=122308; Joe Trevithick, "Learn to Speak Air Force: A Public Service Announcement Regarding Drones," *War is Boring* (blog), 27 May 2014, https://medium.com/war-is-boring/learn-to-speak-air-force-e6ebc5614b25.

[3] This article focuses on "civil society" use of drones. By civil society I mean non-state and non-commercial actors using UAVs for public and private purposes. It is difficult to determine what exactly is meant by the "greater" or "public good," as these definitions are made by individual societies.

[4] Patrick Meier, "Using UAVs for Community Mapping and Disaster Risk Reduction in Haiti," *iRevolution.net*, 9 July 2014, www.irevolution.net/2014/07/09/uavs-for-disaster-risk-reduction-haiti/; Faine Greenwood, "Drones, The Civic Surveillance Equalizer?" *sUAS News*, 24 July 2014, http://www.suasnews.com/2014/07/30184/drones-the-civic-surveillance-equalizer/.

[5] Edward B. Roberts, "What We've Learned: Managing Invention and Innovation," *Research Technology Management* 31, no. 1 (Jan/Feb 1998): 11–29.

[6] John Szarkowski and Eugène Atget, *Atget* (New York: The Museum of Modern Art, New York, 2004); Bonnie Yochelson and Daniel Czitrom, *Rediscovering Jacob Riis: Exposure Journalism and Photography in Turn-of-the-Century New York* (Chicago: University of Chicago Press, 2014).

[7] Philip N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (New Haven, CT: Yale University Press, 2015).

[8] Martin Dodge and Rob Kitchin, *Mapping Cyberspace* (London: Routledge, 2001), ix.

[9] Uri Gordon, "Anarchism and the Politics of Technology," *WorkingUSA* 12, no. 3 (2009): 489–503; Giorel Curran and Morgan Gibson, "WikiLeaks, Anarchism and Technologies of Dissent," *Antipode* 45, no. 2 (March 2013): 294–314.

[10] Curran and Gibson, 299; Murray Bookchin, *The Ecology of Freedom: The Emergence and Dissolution of Hierarchy* (Montreal: Black Rose Books, 1991).

[11] Ibid.

[12] Mark McDonald, "Must All U.S. Embassies Now Be Fortresses?," *New York Times*, 13 September 2012, http://rendezvous.blogs.nytimes.com/2012/09/13/must-u-s-embassies-now-be-fortresses/?_php=true&_type=blogs&_r=0.

[13] I have Patrick Meier to thank for this observation.

[14] Jason Koebler, "A Drone Saved an Elderly Man Who Had Been Missing for Three Days," *Motherboard* (blog), Vice Media, 23 July 2014, www.motherboard.vice.com/read/a-drone-saved-an-elderly-man-who-had-been-missing-for-three-days.

[15] Jeffrey Rayport, "What Big Data Needs: A Code of Ethical Practices," *MIT Technology Review*, 26 May 2011, http://www.technologyreview.com/news/424104/what-big-data-needs-a-code-of-ethical-practices/; Ellen Rooney Martin, "The Ethics of Big Data," *Forbes BrandVoice* (blog), 27 March 2014, http://www.forbes.com/sites/emc/2014/03/27/the-ethics-of-big-data/.

[16] Federal Aviation Administration, "Press Release – FAA to Consider Exemptions for Commercial UAS Movie and TV Production: Seven Companies Petition to Fly Unmanned Aircraft before Rulemaking is Complete," Federal Aviation Administration website, 2 June 2014, http://www.faa.gov/news/press_releases/news_story.cfm?newsId=16294.

[17] "Interview: KATSU and The Graffiti Drone," Center for the Study of the Drone, Bard College, 10 April 2014, http://www.dronecenter.bard.edu/katsu-graffiti-drone; Jacob Kastrenakes, "Graffiti artist KATSU creates abstract paintings using drones with spray cans," *Verge*, 7 April 2014, http://www.theverge.com/2014/4/7/5582128/drone-paintings-by-katsu-graffiti-artist.

[18] For more information, refer to Amnesty International's "Remote Sensing for Human Rights" webpage: http://www.amnestyusa.org/research/science-for-human-rights/remote-sensing-for-human-rights. Additionally, refer to the American Association for the Advancement of Science's Geospatial Technologies and Human Rights Project, online at http://www.aaas.org/page/remote-sensing-human-rights-project. More information can also be found at the Satellite Sentinel Project, online at http://www.satsentinel.org/.

[19] Justin Dougherty, "Firefighters Push To Use Drones For Public Safety," *News9.com*, 12 March 2014, http://www.news9.com/story/24959827/firefighters-push-to-use-drones-for-public-safety.

[20] "Credited for saving life – Draganflyer X4-ES UAS used by RCMP locates unconscious driver after accident," *Draganflyer Innovations, Inc.*, 9 May 2013, http://www.draganfly.com/news/2013/05/10/credited-for-saving-life-draganflyer-x4-es-uas-used-by-rcmp-locates-unconscious-driver-after-accident/; Koebler.

[21] Leo Kelion, "African firm is selling pepper-spray bullet firing drones," *BBC*, 18 June 2014, http://www.bbc.com/news/technology-27902634.

[22] "A New Eye in the Sky: Eco-drones," UNEP Global Environmental Alert Service (GEAS), May 2013, http://www.unep.org/pdf/UNEP-GEAS_MAY_2013.pdf; L.P. Koh and S.A. Wich, "Dawn of Drone Ecology: Low-Cost Autonomous Aerial Vehicles for Conservation," *Tropical Conservation Science* 5, no. 2 (2012): 121–132, http://www.tropicalconservationscience.mongabay.com/content/v5/TCS-2012_jun_121_132_Koh_and_Wich.pdf; "Google Helps WWF Stop Wildlife Crime," World Wildlife Fund, 4 December 2012, http://www.worldwildlife.org/stories/google-helps-wwf-stop-wildlife-crime.

[23] Ibid, World Wildlife Fund.

[24] Sandi Doughton, "Using Drones to Monitor Changes in Environment," *Star*, 21 October 2013, http://www.thestar.com.my/News/Environment/2013/10/21/Using-drones-to-monitor-changes.aspx/; Jennifer Duggan, "China Deploys Drones to Spy on Polluting Industries," *Guardian*, 19 March 2014, http://www.theguardian.com/environment/2014/mar/19/china-drones-pollution-smog-beijing; Lian Pin Koh, "Using Drones for Environmental Research and Spying," *ALERT*, 27 April 2014, http://alert-conservation.org/issues-research-highlights/2014/4/27/using-drones-for-environmental-spying-and-research.

[25] Gitonga Njeru, "Kenya to Deploy Drones in All National Parks in Bid to Tackle Poaching," *Guardian*, 25 April 2014, http://www.theguardian.com/environment/2014/apr/25/kenya-drones-national-parks-poaching.

[26] Jack Chow, "Predators for Peace: Drones have Revolutionized War. Why Not Let Them Deliver Aid?," *Foreign Policy*, 27 April 2012, http://www.foreignpolicy.com/articles/2012/04/27/predators_for_peace.

[27] Mabel González Bustelo, "Drone Technology: The Humanitarian Potential," *Open Democracy*, 3 October 2013, http://www.opendemocracy.net/opensecurity/mabel-gonzález-bustelo/drone-technology-humanitarian-potential-0; Patrick Meier, "Using UAVs for Community Mapping and Disaster Risk Reduction in Haiti," *iRevolution.net*, 9 July 2014, http://www.irevolution.net/2014/07/09/uavs-for-disaster-risk-reduction-haiti/; Lean Alfred Santos, "In the Philippines, Drones Provide Humanitarian Relief," *Devex*, 16 December 2013, https://www.devex.com/news/in-the-philippines-drones-provide-humanitarian-relief-82512.

[28] Louise Roug, "Eye in the Sky: Drones are Cheap, Simple, and Potential Game Changers for Newsrooms," *Columbia Journalism Review*, 1 May 2014, http://www.cjr.org/cover_story/eye_in_the_sky.php?page=all.

[29] Melissa Bell, "Drone Journalism? The Idea Could Fly in the U.S.," *Washington Post*, 4 December 2011, http://www.washingtonpost.com/blogs/blogpost/post/drone-journalism-the-idea-could-fly-in-the-ussoon/2011/12/04/gIQAhYfXSO_blog.html.

[30] Kashmir Hill, "Potential Drone Use: Finding Rivers of Blood," *Forbes*, 25 January 2012, http://www.forbes.com/sites/kashmirhill/2012/01/25/potential-drone-use-finding-rivers-of-blood/.

[31] Twilight Greenaway, "Can Drones Expose Factory Farms? This Journalist Hopes So," *Civileats.com*, 17 June 2014, http://civileats.com/2014/06/17/can-drones-expose-factory-farms-this-journalist-hopes-so/.

[32] Bustelo.

[33] Wesley M. DeBusk, "Unmanned Aerial Vehicle Systems for Disaster Relief: Tornado Alley," NASA Technical Reports Server (NTRS), Conference Paper, Report No. ARC-E-DAA-TN500, 2009, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20090036330.pdf.

[34] Jassem Al Salami, "Drone Battle Over Syria: Loyalists and Rebels Spying on Each Other with Off-the-Shelf Robots," *War is Boring* (blog), 11 April 2014, https://medium.com/war-is-boring/drone-battle-over-syria-159387e9de2b.

[35] Rachel Browne and Alia Dharssi, "'Stunt Headed Nowhere': Activists Decry Plan to Use Drones to Secretly Film Forced Labour in India," *National Post*, 13 December 2013, http://www.news.nationalpost.com/2013/12/13/stunt-headed-nowhere-activists-decry-free-the-slaves-plan-to-use-drones-to-secretly-film-forced-labour-in-india/.

[36] "UN Advisers Invoke 'Responsibility to Protect' Civilians in Syria from Mass Atrocities," UN News Centre, 14 June 2012, http://www.un.org/apps/news/story.asp?NewsID=42235#.VEBdVOd8GeY; Michael Abramowitz, "Does the United States Have a 'Responsibility to Protect' the Syrian People?," *Washington Post*, 6 September 2013, http://www.washingtonpost.com/opinions/does-the-united-states-have-a-responsibility-to-protect-the-syrian-people/2013/09/06/5decf4c0-167d-11e3-be6e-dc6ae8a5b3a8_story.html.

[37] Andrew Stobo Sniderman and Mark Hanis, "Drones for Human Rights," *New York Times*, 30 January 2012, http://www.nytimes.com/2012/01/31/opinion/drones-for-human-rights.html?_r=2&.

[38] Ibid.

[39] Sam Gregory, "Cameras Everywhere: Ubiquitous Video Documentation of Human Rights,New Forms of Video Advocacy, and Considerations of Safety, Security, Dignity, and Consent" *Journal of Human Rights Practice* 2, no. 2 (2010): 191–207.

[40] "Drones Deployed to Capture Footage of Protests in Thailand," *France24 Web News*, 4 Decemeber 2013, http://www.france24.com/en/20131204-thailand-drones-deployed-to-capture-protests/.

[41] Matthew Schroyer, "Interview with a Citizen Drone Journalist in Istanbul: 'I Have Been Witnessing Some Very Bad Things,'" Professional Society of Drone Journalists, 24 June 2013, www.dronejournalism.org/news/2013/8/interview-with-a-citizen-drone-journalist-in-istanbul-i-have-been-witnessing-some-very-bad-things; Matthew Schroyer, "Drone Journalism Over Anti-ACTA Protests in Estonia," *mentalmunition.com*, 13 February 2012, www.mentalmunition.com/2012/02/drone-journalism-over-anti-acta.html; Robert Mackey, "Drone Journalism Arrives," *The Lede Blog, New York Times*, 17 November 2011, http://thelede.blogs.nytimes.com/2011/11/17/drone-journalism-arrives/; BBC, "Hong Kong Protest: Drone Captures Scale of Protest," *BBC*, 30 September 2014, http://www.bbc.com/news/world-asia-29421914; Aaron Sankin, "Should Drones be Allowed to Fly Over Ferguson?," *thedailydot.com*, 17 August 2014, http://www.dailydot.com/politics/ferguson-drone-footage-ruptly-video/.

[42] Sarah A. Soule and Christian Davenport, "Velvet Glove, Iron Fist, or Even Hand? Protest Policing in the United States, 1960-1990," *Mobilization* 14, no. 1 (2009): 1–22.

[43] Ian Steadman, "Turkish Protesters Use a Camera Drone, so Police Shoot it Down," *Wired*, 24 June 2013, www.wired.co.uk/news/archive/2013-06/24/turkish-protest-drone-shot-down.

[44] I have the technologist and inventor John Holland to thank for this observation. Interview on 26 April 2014.

[45] Refer to the Humanitarian UAV Network's website for more information: www.uaviators.org.

[46] Refer to the Drone Journalism Lab's website for more information: www.dronejournalismlab.org.

[47] "Domestic Drones," ACLU *Blog of Rights*, http://www.aclu.org/blog/tag/domestic-drones.

[48] Edited for brevity. Full guidelines available at: http://www.aclu.org/blog/tag/domestic-drones; http://www.dronejournalism.org/code-of-ethics; https://docs.google.com/document/d/1pliYVNek2RsiSQ8_9ATFdJBzYFVP88edfLHL8uFBhUA/edit.

[49] Roug.

[50] Email correspondence with Patrick Meier, 3 August 2014.

[51] Dean Starkman, *The Watchdog That Didn't Bark: The Financial Crisis and the Disappearance of Investigative Journalism* (New York: Columbia University Press, 2014).

[52] "SPJ Code of Ethics," Society of Profession Journalists, http://www.spj.org/ethicscode.asp.

[53] It is worth asking who will protect citizens from the prying eyes of an organized civil society group whose use of UAVs pursues a very narrowly defined agenda to the detriment of the public good. It is likely that this situation would be remedied by appeals to the state.

[54] CAL. PEN. CODE § 647 : California Code - Section 647(i), at codes.lp.findlaw.com/cacode/PEN/3/1/15/2/s647/.

[55] Roug.

[56] Verta Taylor and Nella Van Dyke, "'Get Up, Stand Up': Tactical Repertoires of Social Movements," *The Blackwell Companion to Social Movements*, ed. David Snow, Sarah Soule, and Hanspeter Kriesi (Malden and Oxford, England: Blackwell, 2004), 262–293.

[57] Doug McAdam and David A. Snow, eds., *Social Movements: Readings on Their Emergence, Mobilization, and Dynamics* (Los Angeles: Roxbury, 1997), 326; Philip Howard, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam* (Oxford, England: Oxford University Press, 2010).

[58] Taylor and Van Dyke misattribute this statement to Rochon (1998) on page 264.

[59] Ron Eyerman, "The Role of the Arts in Political Protest," *Mobilizing Ideas*, 3 June 2013, http://mobilizingideas.wordpress.com/2013/06/03/the-role-of-the-arts-in-political-protest/; "FAA Selects Six Sites for Unmanned Aircraft Research," FAA, http://www.faa.gov/news/updates/?newsId=75399.

[60] "April 12 Event Will Put Drone Skills to the Test," North Carolina State University, 26 March 2014, http://news.engr.ncsu.edu/2014/03/april-12-event-will-put-drone-skills-to-the-test/.

[61] See www.irevolution.net.

[62] An example of this broader range of actors would include Amnesty International's launch of the Eyes on Darfur campaign.

[63] See the Satellite Sentinel Project, http://www.satsentinel.org.

[64] Patrick Meier, "The Use of Drones for Nonviolent Civil Resistance," *iRevolution.net*, 18 February 2012, http://irevolution.net/2012/02/18/drones-for-civil-resistance/.

[65] Ibid.

[66] Aaron Smith, "U.S. Views of Technology and the Future: Science in the Next 50 Years," *Internet & American Life Project*, Pew Research Center, 2014, http://www.pewinternet.org/2014/04/17/us-views-of-technology-and-the-future/.

[67] Leon Watson, "Woman Claims She was Sexually Harassed by a Drone After Catching Man Flying Remote-Controlled Plane at the Beach that got Uncomfortably Close to Female Sunbathers," *Daily Mail*, 15 May 2014, http://www.dailymail.co.uk/news/article-2629459/Woman-claims-sexually-harassed-DRONE-catching-man-flying-remote-controlled-plane-beach-got-uncomfortable-close-female-sunbathers.html#ixzz34FEL.npg; Jason Koebler, "This Kid Got Assaulted for Flying His Drone on a Beach," *Motherboard* (blog), Vice Media, 9 June 2014, http://motherboard.vice.com/read/this-kid-got-assaulted-for-flying-his-drone-on-a-beach.

[68] Jason Koebler, "African Nations Are Banning the Drones That Could Stop Poachers," *Motherboard* (blog), Vice Media, 4 June 2014, http://motherboard.vice.com/read/african-nations-are-banning-the-drones-that-could-stop-poachers.

[69] "Drones Banned in South Africa," *Times Live*, 3 June 2014, http://www.timeslive.co.za/scitech/2014/06/03/drones-banned-in-south-africa.

CONTRIBUTORS

Burcu Baykurt is a doctoral candidate in communications at Columbia University's Graduate School of Journalism where she studies the effect of technological change on the cultures of journalism, politics, and public policy. Before Columbia, she studied political communications at Goldsmiths, University of London and holds a master's degree in Media, Culture and Communication from New York University.

Pavin Chachavalpongpun is an associate professor at the Center for Southeast Asian Studies, Kyoto University, Japan. Earning his PhD from the School of Oriental and African Studies at the University of London, Pavin is the author of two books: *A Plastic Nation: The Curse of Thainess in Thai-Burmese Relations* and *Reinventing Thailand: Thaksin and his Foreign Policy*. He is also the editor of the recently released *Good Coup Gone Bad: Thailand's Political Developments Since Thaksin's Downfall*. Pavin is the editor of the online journal *Kyoto Review of Southeast Asia* and teaches politics of Southeast Asia, and in particular Thailand, at the graduate level. In the wake of Thailand's 2014 coup, Pavin was critical of the military's intervention methodologies. As a result, the Thai junta ordered him to report to them, twice. Publicly denying the legitimacy of the coup, he ignored the orders, and ultimately, the junta issued a warrant for his arrest and revoked his passport. He was granted refugee status in Japan, where he currently resides.

Austin Choi-Fitzpatrick is an assistant professor of political sociology at the School of Public Policy at Central European University, an American graduate school in Budapest, Hungary. He is currently working on two projects. The first is related to contemporary slavery and includes a number of articles, an edited volume with the University of Pennsylvania Press's series on Human Rights, and a book manuscript on social movement targets. The second project emphasizes civil society's use of drone technology through an innovative campus-based Drone Lab. The lab's first major project is a drone-based method designed to more accurately estimate the size of protest events.

Michael C. Davis is a professor in the law faculty at the University of Hong Kong. He has held visiting chairs in human rights at Northwestern University

Eyes in the Sky

Will drones end privacy as we know it?

by Edward Humes | August 2013

Drone illustration by Paul Fleet; background photo by franckreporter.

Related Articles

Dilemmas of State: A Conversation with Harold Koh
November 2012

Vive What Différence?
July 2011

Comment
ShareThis
Print
Reprint

Like many people who post their vacation videos on YouTube, Raphael Pirker offers plenty of clips of familiar, touristy landmarks. But instead of the usual parade of postcard poses and frozen grins, Pirker - a.k.a. *nastycop420* - draws huge online crowds with gravity-defying flybys and fly-throughs. In one of his videos, he shoots high above the Golden Gate Bridge, then suddenly pivots into a stomach-wrenching dive that takes the viewer underneath the span and out again, just above the white-capped waters. In the video, Pirker also shares a barrel-rolling, bird's-eye view of the Hoover Dam, a desert terrain-skimming cruise through red-hued Monument Valley, and a roller coaster loop around the Statue of Liberty's torch, above gawking tourists on the ground.

These aerial acrobatics show off what Pirker can do with the small, camera-equipped drones that he designs, builds, and sells. They show as well how far Pirker is willing to go to defy the Federal Aviation Administration, which restricts the recreational use of drones to unpopulated areas and very low altitudes, and bans their commercial use altogether.

"The U.S. drone rules are essentially unenforceable," says Pirker, who, as part of an informal group of drone enthusiasts known as Team BlackSheep, sells unmanned aircraft from his home base in Hong Kong. (Depending on the range of the custom video-streaming transmitter, prices can run as high as $3,500.)

"This is what we do for fun," he adds. "But we also do it to demonstrate the many uses of this technology - and to expose the holes in most [countries'] regulations."

It's hardly a matter of dispute that the FAA needs to craft new rules on drones. What's less clear, though, is whether the agency will be able to meet a congressionally mandated 2015 deadline. It's a complex task, to be sure. As the FAA estimates, as many as 30,000 of these unmanned flying machines could be licensed in the United States for nonmilitary purposes in less than 20 years. That would include everything from the two-pound wonders that Pirker flies to the airliner-size, pilot-free transoceanic cargo planes that companies such as Federal Express are eager to deploy.

Air safety and traffic are the FAA's primary focus, but concerns about drone use don't stop there. Civil rights advocates worry that law enforcement's use of tiny drones - easily equipped with night-vision capabilities and directional microphones - could stretch the "in plain sight" doctrine to an absurd degree, and in the process end privacy as we know it. On the other hand, journalists argue that restricting the public's use of this rapidly evolving technology could threaten the press's First Amendment right to gather and disseminate news. And as the courts begin to weigh in on these issues, it's anyone's guess how well current stalking, peeping, and wiretapping laws can check the proliferation of drones over the United States.

Do Pirker's pint-size devices portend pervasive police searches, unstoppable robo-paparazzi, and flying spybots - which already can be purchased online for a few hundred dollars? "No matter what happens next," predicts Matt Waite of the University of Nebraska's Drone Journalism Lab (which studies both the practical uses of drones in journalism and the legal and ethical issues they pose) "everybody is going to sue everybody."

California is one of the world's major centers for drone research, and therefore a natural place for these debates to play out. Among its leading defense contractors is San Diego's General Atomics Aeronautical Systems, maker of the missile-equipped Predator, often used to take out suspected militants in Afghanistan, Pakistan, Yemen, and elsewhere. In Ventura County, AeroVironment specializes in smaller observer drones. Lockheed-Martin, Boeing, and Raytheon, which maintain

operations in California, each have a piece of the military drone market as well. Meanwhile, smaller companies such as 3D Robotics, a San Diego start-up, are building inexpensive drones for the hobbyist market. In Washington, D.C., 7 of the 50 representatives who belong to the House Unmanned Systems Caucus, cochaired by U.S. Rep. Howard "Buck" McKeon (R-Santa Clarita), are Californians. And it's widely anticipated that the Golden State will soon host one of six national drone test sites to help the federal government determine how to integrate drones into our domestic airspace.

California figures prominently too in the legal history of aerial snooping. In 1986 the U.S. Supreme Court held in *California v. Ciraolo* (476 U.S. 207) that police could legally spy on private property from an aircraft without warrants. The high court, however, has hinted that it may look differently on searches conducted by stealthier, highly maneuverable drones that can be deployed far more cheaply - and therefore pervasively - than piloted aircraft.

"The technology is rapidly evolving and very easily abused," says Linda Lye, staff attorney for the American Civil Liberties Union of Northern California, which sharply objected to a recent draft policy prepared by the Alameda County Sheriff's Department on drone usage. "It's vital that the law keep up," Lye adds.

But what, exactly, does keeping up mean, if the goal is to curtail the possible abuses of drone technology while also trying to aggressively exploit its potential in such areas as farming, firefighting, and search-and-rescue operations? At this point, no one really knows.

We basically take cell phones and give them wings and propellers, and use them as data-acquisition devices," says Chris Anderson, formerly the editor of *Wired* magazine. Now, as the CEO of 3D Robotics, he sells about a thousand drones or drone guidance systems a month, starting at about $600 apiece.

Another high-flying entrepreneur who is bullish on drones is Patrick Egan of Sacramento. Prior to February 2007, he claims, he was making up to a thousand dollars a day using drones to photograph high-rise condos and other properties for real estate agents and corporate clients. But after he drew attention to himself by publicly questioning the FAA's rules, the agency ordered him to shut down his business until the FAA could issue new rules. That was six years ago.

"It all seems very arbitrary and capricious," says Egan, who can't help but notice that others with lower-profile operations continue to do commercial real estate photography with drones.

For regulatory purposes, the FAA splits the domestic drone market into three distinct categories: civil, public, and recreational. The civil side consists primarily of commercial drones flown for profit, which have never been flown legally in the United States, and five experimental certificates granted by the FAA for research and training. Doing business with drones will remain officially banned until at least 2015, when the FAA is supposed to issue new standards for pilots, registration, licensing, and onboard sensory and collision-avoidance technology.

Once these standards are in place for civil drones, public-agency drones will undoubtedly have to follow similar safety and certification standards. But for now, public-drone flights can be authorized on a case-by-case basis under limited range, altitude, and operating restrictions through special FAA certificates of authorization (COA).

More than 1,400 of these COAs have been issued since 2007, and 327 remain active. Most of the 10 that are active in California are held by universities or military bases. Law enforcement agencies have also expressed an interest in applying for COAs. And, in fact, just two months ago FBI Director Robert Mueller told a Senate committee that his agency has used drones in domestic surveillance.

To date, only one arrest has occurred on American soil in which it was publicly acknowledged that drone surveillance played a key role. That was in North Dakota in 2011, when Nelson County authorities investigating suspected cattle thieves they believed were armed and dangerous received assistance from a Predator drone. Sheriff Kelly Janke said the Predator overflight - which would not have required a warrant if performed by a piloted craft - helped deputies stage a safe, nonviolent arrest.

As for those who fly drones purely for fun, they are subject to FAA hobbyist rules that were originally developed as voluntary guidelines for model airplane enthusiasts back in 1981. The regulations cover all model aircraft that are not flown for profit. According to FAA Advisory Circular 91-57, recreational drones are supposed to operate within 400 feet of the ground, remain within sight of their operators at all times, and steer clear of airports, other air traffic, and populated areas. But, as Pirker's videos clearly show, these restrictions aren't always adhered to.

Pirker maintains that the FAA's rules are merely "advisory," and that they lack the force of law so long as operators fly in what he describes as a "safe manner." But, of course, the FAA doesn't see it that way, and in June the agency issued a $10,000 fine against Pirker for various regulation infringements, including operating a drone, or unmanned aircraft system (UAS), "in a careless or reckless manner, so as to endanger the life or property of another." Pirker says he cannot afford, nor will he pay, the fine, and he continues to deny wrongdoing.

Others, too, are receiving unwanted attention from the feds. Among them, News Corp's now-shuttered tablet-format news website, *The Daily*, which drew a cease and desist order last year when it used a drone to gather aerial footage for a report on tornado devastation in the Midwest. And though independent filmmaker Patrick Gilles used a drone to shoot some scenes for his 2011 movie, *Olive*, in his next film he's decided to stay on the right side of the law, even though it means he now has to shoot the film's aerial scenes from a helicopter, which is not only more expensive but more dangerous as well.

In addition to what the feds are doing to deter drone use, state and municipal officials seem

determined to draft their own domestic-surveillance drone laws - even though federal regulations could preempt many of those measures. The ACLU reports that no fewer than 42 states have considered regulations or restrictions on drones, with preservation of privacy being the prime concern. Florida, Idaho, Montana, and Tennessee already require search warrants in most cases before police can use drones, and Virginia police have been barred from using drones with or without warrants for the next two years.

Texas, on the other hand, is going in a very different direction. In June its governor, Rick Perry, signed into law a bill that goes into effect next month, which allows law enforcement officials to use drones for surveillance if they have "reasonable suspicion" of criminal activity. The law also makes it a misdemeanor for most private drone owners to fly their craft over private property without permission. This legislation, by the way, was drafted after a hobbyist's drone inadvertently showed a meatpacking plant illegally polluting a river.

In California, the state Senate recently passed a bill (SB 15) that would expand existing criminal and civil penalties for invasion of privacy, eavesdropping, and peeping when drones are involved. The bill also would require search warrants when police use drones for surveillance of people or property that would otherwise require warrants.

At a recent committee hearing, state Sen. Alex Padilla (D-Pacoima) explained that the goal of his bill is to add drones to existing privacy and search warrant statutes. "We need look no further than the Boston Marathon [bombings in April] to just imagine what someone with nefarious intent could do with technology like this," he said. "So in the absence of any regulatory structure, we do need something in place."

Padilla's bill would also ban drones in California from carrying weapons.

The drones Americans know best, of course, are the San Diego-built Predators. These massive, hawk-billed birds, costing $4 million apiece, are designed to conduct long-range remote surveillance and rain Hellfire missiles down on far-flung targets. As sophisticated as these killing machines are, though, when it comes to developing this technology for civilian applications the United States lags well behind much of the rest of the world.

As far back as the late 1980s, Japanese farmers were using unmanned helicopters for crop dusting. The Australians too are moving forward. A decade ago the government began licensing drone operators for aerial photography, surveying, and media coverage of sporting events. And now there are proposals on the table to further expand the use of drones.

But in this country, it's only since the wars in Iraq and Afghanistan started to wind down that domestic applications have been more broadly considered. One company that is looking for new markets is AeroVironment. After seeing its annual revenues for military drones shrink by almost a third last year, the company began assessing both emergency responders and law enforcement as potential sources of business. "The possible uses of this technology are extremely broad," says Steven Gitlin, who is the company's vice president of marketing strategy and communications. But law enforcement, he adds, is "a logical first step."

Not everyone would agree. Mark Corcoran, a drone researcher at Sydney's University of Technology in Australia, believes the FAA made a major tactical blunder when it singled out law enforcement as the first domestic drone application in the United States to be phased in. "Had the FAA first permitted the demonstration of more positive civilian applications of drone technology," Corcoran ventures, "I doubt that there would have been such an intense privacy debate."

Indeed, the feelings that Americans have about drones these days are so negative that whenever the head of the drone industry's largest trade group, Michael Toscano, talks about the technology, he tends to avoid using the "d" word.

"The unmanned-systems opportunity is enormous - to reduce costs, lower risks," said Toscano, president and CEO of the Association for Unmanned Vehicle Systems International, at a drone conference in Thousand Oaks, California. "We have to avoid creating legal hurdles that can destroy this opportunity."

For the purposes of regulation, Toscano says, "Both [manned and unmanned aircraft] involve a plane and a camera. There's no real difference."

"They're *not* the same," counters Lye of the ACLU. And one of the most important differences, she says, is cost. "Drone surveillance is becoming so inexpensive that it could lift a practical barrier to what has been a [legal] barrier to abuses."

Lye suspects, moreover, that the U.S. Supreme Court may be coming around to her point of view. In last year's case of *People v. Jones* (132 S. Ct. 945 (2012)), she notes the high court ruled unanimously that attaching a GPS device to a suspected drug trafficker's car constituted a search under the Fourth Amendment. Obviously, planting a tracking device underneath a car is not at all the same as recording a suspect's movements with a drone. But in a concurring opinion joined by three other justices, Justice Samuel A. Alito reflected on the impact of technology that is both inexpensive and potentially invasive. "In the pre-computer age," Alito wrote, "the greatest protections of privacy were neither constitutional nor statutory, but practical. ... Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."

However, at Pepperdine University associate law professor Gregory S. McNeal characterizes privacy concerns about drones as "somewhat overwrought." He also thinks the ACLU's proposal for warrant requirements are problematic and will lead to troubling inconsistencies. For example, he notes that a crime automatically recorded by a police car's dashboard camera is admissible in court. But were a drone to capture the same footage without a warrant, it would be inadmissible under the ACLU's proposal.

The best way to deal with these issues, says McNeal, is through public transparency and reporting requirements. "Then, if you found out that some officer likes to fly his drone near a sorority house with the camera always pointed in its direction, at the end of the month, when the logs are made, the public will see what he's doing and he'll have to stop."

Transparency is a goal that drone enthusiast Pirker can warm up to, as well. After all, when it comes to flying drones, no one is more "out there" than he is.

"Our [two-pound models] are nothing like the big military drones," he says. "They can't hurt anything. With some commonsense rules and some training, the safety issues can be resolved - and then the sky's the limit."

Edward Humes, based in Southern California, is a Pulitzer Prize-winning journalist and author of twelve nonfiction books.

DRONES DEFINED: What's a drone?

A deceptively simple question begets an increasingly complex answer. Once known solely as a weapon of war, the term drone now also covers the ten-pound, auto-piloted aircraft your nerdy neighbor just built in his garage. It might look like the model airplanes of your youth, but chances are the technology is different.

The fact that one term applies to both recreational and killer aircraft illustrates just how much the definition of a drone has evolved. In short, a drone (either an unmanned aerial vehicle (UAV), or unmanned aerial system (UAS), as it is less-threateningly referred to by government agencies and politicians alike), is any aircraft capable of autonomous flight. A GPS system is commonly in place to guide the aircraft, and often drones are equipped with cameras, infrared devices, microphones, or other sensors, sometimes even with lasers. Drones also can wirelessly transmit information back to their operator, or home base. They can be as compact as a small bird (Nano Hummingbird) or as large as a fighter jet (X-47B). *-Logan Orlando*

Reader Comments

Concerned Victim - February 7, 2014
It's already happening in California, Drones are being used to perform illegal searches on individuals inside their homes. To be more precise they are being used around Travis Air Force Base in Napa, American Canyon, Vallejo, Concord, Antioch, Oakley, and Brentwood. Not sure yet who controls them, however they are definitely being used by Napa and Contra Costa County officials. The scans can not only be heard but can be felt like a sound of a stereo with a strong base system going thru ones body. Several individuals have been scanned in their own homes or while visiting friends homes in Vallejo, Napa, American Canyon, Oakley, and Antioch. After feeling the scan they have gone outside to see what might be causing it and everytime their has been an unmanned ariel vehicle in the sky or lights low in the sky at night which fly away to avoid detection, or maintain a pattern in the sky such as the constillation "Orion's Belt" to avoid detection. Whomever is controlling them knows very well that they are deliberately defying these individuals rights to privacy and avoid being "caught" by a cameras view. Some have tried to attain an attorney but have been advised that such a case would demand an extensive investigation which in turn would cost more than most could afford to retain such a service to be able to follow through to a court of law. That being said. it is way too easy for "officials" to abuse this power and way to hard for most of us to "prove" in a court of law! So we just loose our right to expect privacy in our homes? We all become victims to un-authorized and illegal searches? We all fall victim to being viewed within the walls of our homes? In our bedrooms? In our bathrooms? Believe me they already have this technological ability and they are already abusing it! If you don't believe it, just look in the skies around Napa junction any night or day of the week, especially in the neighborhoods surrounding the all night super Walmart at Napa Junction, perhaps, should you look the type you might even be scanned while shopping? Its happened to some of us already and it appears that most of the community protect the drones and their controllers, because if you start flashing a camera in public they will alarm them with their horns or car alarms and the drones will disappear suddenly behind the apartments, clouds, trees, or if its night time a helicopter might suddenly appear in the sky so you are detoured from using a flash. The scan of the drones at times is so strong that individuals while being scanned feel light headed, dizziness, nauseous and "equilibrium feels off balance. Once they are out of the drones scan they feel normal almost immediately, depending on the frequency and number of scans they've encountered in a day. Some have left with the off balance feeling (similiar to a drunken state) for several hours after being scanned. So What Now? How can this type of abuse be stopped? Sherrifs' dept. claims they have no drones, so how does one go about pursuing justice when they cant find whom is responsible for the actions of these drones, other than their is always someone near them signaling the drone where to scan, how do we find or begin to find the party(s) responsible, in order to seek justice?

Bob Smith - February 8, 2015
I think you are describing a UFO encounter, you nut job!!!

We welcome your comments!

Name

E-mail: (will not be published)

By submitting a comment, you agree to abide by our comment policy.

Enter the characters on the left:

Submit Comment

Title: Privacy in the age of Big Data
Author(s): John Pavolotsky
Source: ***Business Lawyer.*** 69.1 (Nov. 2013): p217.
Document Type: Article

http://www.abanet.org
Full Text:

"Big Data" is here. In fact, soon Big Data will be small data. (1) Gartner defines Big Data as "high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making." (2) In essence, Big Data refers to the proliferation in data volumes and types, the dramatic increase in the speed for collecting and processing that data, and the technical solutions to analyze, store, and draw intelligent and actionable inferences from the data. Big Data is premised on intensive data mining on large and diverse data sets, which may be online, offline, or a combination of the two. The rise in unstructured data (free-form text, video, voice, etc.) and machine data (web, server, application, and database logs; sensor data from medical devices, smart meters, and appliances), cheaper storage, web services, and the ubiquity of broadband access in many corners have all played a large role in the emergence of Big Data. Technical solutions include Apache Hadoop, (3) an open source software platform that enables, among other things, the parallel processing of large data sets. Big Data and related technologies have been applied in a number of industries, including retail, (4) healthcare, (5) insurance, (6) automotive, (7) entertainment, (8) and publishing. (9) More ominous applications include cell- phone tracking, (10) the proposed creation of a national biometric database, (11) and drones. (12) Thus, while Big Data creates many benefits, it raises a number of issues, including those relating to data privacy. This survey focuses on the privacy issues raised by Big Data and suggests risk mitigation techniques.

I. BIG DATA JURISPRUDENCE

At a minimum, courts are beginning to acknowledge Big Data. For example, one court noted: "First, in the era of 'big data,' in which storage capacity is cheap and several bankers' boxes of documents can be stored with a keystroke on a three inch thumb drive, there are simply more documents that everyone is keeping and a concomitant necessity to log more of them." (13) Another court noted that a certain Big Data analytics market "consists of companies that use data mining techniques to derive insights from the flow of information generated on" a particular social networking site. (14) As discussed below, other courts, while not using the term Big Data, have nonetheless tackled issues, such as geolocational privacy, raised by Big Data technologies. In particular, these courts have examined the collection and use of GPS data, from both traditional GPS transponders and GPS chips in mobile phones, and cell site data by law enforcement officials in connection with surveillance operations.

United States v. Jones (15) involved a GPS device that had been attached to the undercarriage of the defendant's car. The GPS device tracked the location of Mr. Jones's car for twenty-eight consecutive days, relaying more than 2,000 pages of data. (16) While Justice Scalia's majority opinion ultimately disposed of the case based on a common law trespass analysis, (17) Justice Alito, in a concurring opinion joined by three other Justices, provided that prolonged monitoring of a person's whereabouts for most offenses would violate a person's reasonable expectation of privacy and, therefore, be unconstitutional, absent a warrant or exigent circumstances. (18) Although Justice Sotomayor penned a separate concurring opinion, she nonetheless seemed to agree with Justice Alito's reasoning. (19) In view of the foregoing, it seems likely that the Court will continue to apply the "reasonable expectation of privacy" test first articulated by Justice Harlan in Katz v. United States (20) to tracking technologies. Further, relatively recent advancements in tracking technologies, which allow location data to be collected without attaching a physical device to the property of the person being tracked, call into question the utility of a common law trespass analysis in future cases.

United States v. Skinner (21) involved a GPS-enabled cell phone that was pinged periodically for three days. Law enforcement officials used location data collected from the phone to apprehend the defendant, who subsequently filed a motion to suppress, arguing that a warrant based on probable cause should have been obtained before any data were gathered. (22) The U.S. Court of Appeals for the Sixth Circuit concluded that "Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." (23) While Judge Donald, in her concurring opinion, disagreed with the majority's rationale, she nonetheless concluded that the location data evidence should not be suppressed because a good-faith exception to the warrant requirement existed. (24)

Courts have also examined the constitutionality of warrantless searches based on the collection of cell-site data. Put simply, wireless carriers record the locations of the nearest cell towers at the beginning and end of a phone call made on a mobile device. (25) With such data, the location of a device can be determined with reasonable accuracy. (26)

Interestingly, relying on the Court's favorable ruling in United States v. Jones, (27) Mr. Jones petitioned the U.S. District Court for the District of Columbia to suppress cell-site data gathered during a four-month period pursuant to three separate orders issued by magistrate judges. (28) In particular, Jones argued that such data could not be collected without a warrant based on probable cause. (29) There, the court denied the defendant's motion to suppress, because, in its view, the good-faith exception to the exclusionary rule applied. (30) Notably, the court discussed in great detail the constitutionality of collecting cell-site data without a warrant based on probable cause, but, as noted above, was able to avoid a determination because "exclusion is not required 'when the police act with an objectively reasonable good-faith belief that their conduct is lawful.'" (31)

II. BIG DATA AND FIPs

For most practicing attorneys, the issues raised by government surveillance cases are of limited applicability, but the issues loom large for any practitioner who represents the government, the defendant whose location data have been collected by law enforcement officials, or a state actor. While other attorneys need not face these issues, they still must be aware of the privacy issues, as detailed below, raised by Big Data.

As noted, Big Data is founded on comprehensive data collection and extreme data analytics, which guide the use and/or disclosure of the data. Modern privacy law is based on fair information practices (FIPs), principles that address the rights of individuals, controls on the information, and the collection, use and storage, and disclosure of the information. (32) Individuals' rights consist of notice, choice and consent, and access. (33)

Notice and consent are problematic, particularly so for Big Data. Many consumers do not read privacy policies, which are often inscrutable to lawyers and non-lawyers alike. Privacy policies displayed on devices, such as cell phones, with small-form factors are at best difficult to read, and layered notices, providing a brief summary of the privacy terms with a link to the full privacy policy, are often unavailable. Notices should be clear and state the purpose for which personal data will be collected, used, disclosed, and retained. In the case of Big Data, prospective identification of the data-collection purposes may be challenging because an organization cannot realistically anticipate what the data will reveal until after intensive data mining is complete.

Put otherwise, even if an individual read and understood a privacy policy, that policy may be wrong or at least incomplete. Again, Big Data, the value of which lies in identifying secondary (and thus unimagined) uses of data, stretches the practical limits of meaningful consent. Moreover, the entity collecting data may transmit it to another, thereby losing control over its ultimate use. Further, a direct relationship might not exist between a data subject and the organization that stores his or her personal information. Consider, for example, data brokers, which collect, combine, and sell (or license) data from online and offline sources for marketing and other purposes. (34) In practical terms, individuals would have no way of knowing who ultimately uses their data or how it ultimately might be used.

III. ANONYMIZATION

One of the foundational concepts in modern privacy law is anonymization or de-identification. (35) As applied to data, this involves masking or obfuscating data to prevent individual identification. In the European Union, personal data relates to an identified or identifiable individual. (36) If data is effectively anonymized, the EU Data Protection Directive would not apply. (37) The same concept applies to U.S. data privacy laws, such as the Health Insurance Portability and Accountability Act of 1996 (38) and, in particular, the Privacy Rule thereunder, the latter of which allows de-identification of personal health information through an "Expert Determination" method (which requires the application of statistical or scientific principles to determine the risk of identification) and "Safe Harbor" method (which involves removing eighteen types of identifiers and requiring the absence of actual knowledge that the information could be used to identify an individual). (39) In addition, to comply with state data breach statutes, (40) organizations routinely obfuscate data. Big Data and related techniques challenge and in some instances re-identify previously de-identified data. Put simply, with the availability of even bigger data sets and more robust analytics, there are sometimes only a few hops between de-identified data and the identity of a particular individual. For example, researchers at MIT and the Universite Catholique de Louvain (Belgium) analyzed data on 1.5 million cellphone users residing in a small European county and found that they could identify 95 percent of such users based on only four points of reference. (41) Thus, the Big Data tsunami should prompt companies to review their de-identification protocols, ensure that these protocols are being implemented properly, and reconsider if certain data should simply not be collected from individuals.

IV. THE FTC AND BIG DATA

A. DATA BROKERS

The Federal Trade Commission ("FTC") has been active in pursuing data brokers regarding potential privacy issues and, in particular, potential violations of the Fair Credit Reporting Act ("FCRA"). (42) On May 7, 2013, the FTC announced that it recently had conducted a "shopping operation," showing that a number of companies may be operating as consumer reporting agencies and, as such, would be subject to the FCRA. (43) In particular, the FTC sent letters to ten such companies, noting potential violations, including failures to confirm that the purchasers of the consumer lists and other consumer reformation offered by these data brokers would use them only for permissible purposes. (44) Clearly, the FTC is setting the stage for a long battle with data brokers. (45) Previously, and to no avail, the FTC had called for legislative oversight of data brokers and, in particular, legislation to require data brokers to identify to individuals whether personal data are held by them with respect to the individuals. (46) In 2012, the FTC announced that, for $800,000, it had settled claims that Spokeo, a data broker that compiles and sells reformation profiles, operated as a consumer reporting agency and violated the FCRA by, among other things, failing to ensure that the profiles were used for lawful purposes. (47)

B. PRIVACY BY DESIGN

While Privacy by Design ("PBD") is not a new concept, it was expressly and fully embraced by the FTC in its 2012 report titled Protecting Consumer Privacy in an Era of Rapid Change. (48) In essence, PBD provides that organizations, at every stage of a product's design and development, should build in consumer privacy protections, such as reasonable security, limited data collection and retention, and reasonable procedures to achieve data accuracy. (49) In February 2013, a leading mobile device manufacturer settled FTC charges that it failed to use reasonable security practices when it developed software for its smartphones and tablets. (50) The resulting security flaws, in the FTC's view, could have put at risk sensitive information about millions of customers. (51) Notably, while charges relating to security were asserted under the unfairness prong of section 5 of the FTC Act, (52) clearly the FTC had PBD in mind when prescribing the proactive implementation of reasonable data security measures. (53) The importance of data security is heightened by the volume of data collected, as well as by the nature of the data. Thus, Big Data technologies and practices should stress PBD and cause any organization to think twice about what personal data it collects, how it secures that data, and how it can integrate robust security protections as the product is being designed and developed.

C. DO NOT TRACK

While Do Not Track ("DNT") is at the top of the FTC's agenda, (54) given disagreements regarding technical implementation and continuing debate over the value proposition for Big Data at the consumer level, it is unlikely that there will be any progress with any DNT legislation anytime soon. Put simply, DNT would be a federally mandated opt-out regime as applied to an individual's search and other internet activities. (55) Note that DNT generally focuses on tracking and not on the underlying collection of consumer data. Put otherwise, even if DNT legislation were passed in some form, there would still likely be massive amounts of data collected, which, as noted above, presents considerable security concerns.

V. PROPOSED LEGISLATION

Not surprisingly, members of Congress have introduced a variety of bills that attempt to deal with the privacy issues raised by technologies that fall within the realm of Big Data. For example, on September 12, 2012, Representative Markey introduced the Mobile Device Privacy Act. (56) Pursuant to this proposed legislation, which has since died, organizations would have needed to disclose monitoring software installed on a mobile device or downloadable to such a device, the types of information that could be collected by such software, the recipients of such information, how such information would be used, and procedures to stop further collection of such information. (57) Further, the bill had somewhat detailed information security requirements for anyone that receives information collected by monitoring software, including a security policy, the identification of a security officer, and a process for identifying any reasonably foreseeable vulnerabilities in any system containing such information. (58) More recently, proposed legislation includes the Electronic Communications Privacy Act Amendments Act of 2013, (59) which was introduced by Senator Leahy. More broadly, Congress is concerned about the requirements for seeking geolocational data and drawing a distinction, if warranted, between particular tracking technologies, namely GPS and cell-tower data. (60)

VI. RISK MITIGATION

In view of the Big Data tsunami, what options are available to organizations to steer clear of potential violations of data privacy laws and for consumers to ensure that reasonable expectations of privacy are in fact being met? For organizations, risk mitigation begins with the development of a comprehensive and realistic privacy plan. In contrast to a privacy policy, a privacy plan is directed internally toward those in the company who will have access to consumer data. Organizations should embrace Privacy by Design, and many have already subscribed to its tenets, by setting privacy as the default.

Companies should devote greater attention to the development of privacy policies that are simpler and more specific to actual products or services and an organization's collection, use, disclosure, and storage of data in connection with that product or service. Put otherwise, because no two businesses are the same, if privacy policies are the same or substantially similar, at least one of the privacy policies is not on point. Big Data and related technologies should cause organizations to refocus their attention on the flow of data in connection with a specific product or service, and if the collected data is to be used for a context different from, or incompatible with, the one for which it was first collected, the consumer should be required to consent to that new use. Ultimately, the notice-and-consent model is based on control, and a consumer cannot control what she or he does not know or cannot reasonably understand.

The situation for organizations using or providing Big Data solutions to other companies is quite different. Business customers, depending on negotiating power, can in many instances have the relevant contract override any otherwise applicable Terms of Service or Privacy Policy documents posted on the service provider's website. Customers can mitigate risk by performing business, technical, and legal due diligence on the Big Data solution. As a practical matter, in many instances, the provider will not accept any liability for personal data and will require the customer to indemnify it if any personal data are provided to it, whether intentionally or inadvertently. The only options for the customer are to encrypt the personal data or to scrub the data, which may present an issue operationally. In practice, whether a vendor accepts any liability for data privacy or security is ultimately a function of negotiating power. While an indemnity is preferable, a damages claim may suffice, so long as it is not subject to a limitation of-liability cap, and it is expressly provided that the vendor is responsible for all notification and remediation costs associated with the breach.

Other risk mitigation options include professional liability insurance with cyber-security coverage. Practitioners should also consider proposing periodic data audits to ensure that the data is being processed, transferred, stored, destroyed, and, in some cases, as necessary, retained, consistent with the customer's litigation hold policies.

(1.) See Patrick Tucker, Has Big Data Made Anonymity Impossible?, MASHABLE (May 7, 2013), http:// mashable.com/2013/05/07/big-data-anonymity/ (noting a 2,000 percent projected increase in global data by 2020).

(2.) Svetlana Sicular, Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s, FORBES (Mar. 27, 2013, 8:00 AM), http://www.forbes.com/sites/gartnergroup/2013/03/27/ gartners-big-data-definition-consists-of-three_parts_not _to_be_confused_with_three_vs/.

(3.) See APACHE HADOOP, http://hadoop.apache.org/(last visited Aug. 25, 2013).

(4.) See Jeff Bertolucci, Big Data Helps Retailers Target Mobile Customers, INFO.WEEK (Apr. 4, 2013), http://www.informationweek.com/big-data/news/big-data-analytics/big-data-helps- retailers-target-mobile-c/240152281.

(5.) See John Markoff, Unreported Side Effects of Drugs Are Found Using Internet Search Data, Study Finds, N.Y. TIMES (Mar. 6, 2013), http://www.nytimes.com/2013/03/07/science/unreported_side_effects_ of-drugs-found-using-internet-data-study-finds.html?_r=0.

(6.) See Clint Boulton, Auto Insurers Bank on Big Data to Drive New Business, WALL ST. J. (Feb. 20, 2013, 5:03 PM), http://blogs.wsj.com/cio/2013/02/20/auto-insurers-bank-on-big- data-to-drive-new-business/.

(7.) See Derrick Harris, How Data Is Changing the Car Game for Ford, USA TODAY (Apr. 29, 2013, 9:36 AM), http://www.usatoday.com/story/tech/2013/04/29/data-ford- gigaom/2120481/.

(8.) See David Carl Giving Viewers What They Want, N.Y. TIMES (Feb. 24, 2013), http://www.nytimes. com/2013/02/25/business/media/for-house-of-cards-using-big-data-to- guarantee.its-popularityhtml? pagewanted=all&_r=0.

(9.) See Alexandra Alter, Your E-Book Is Reading You, WALL ST. J., July 19, 2012, at D1, available at http://online.wsj.com/article/SB10001424052702304870304577490950051438304.html

(10.) See, e.g., United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

(11.) See David Kravets, Biometric Database of All Adult Americans Hidden in Immigration Reform, WINED (May 10, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/05/immigration-reform-dossiers/.

(12.) See Robert Beckhusen, White House 'Big Data' Push Means Big Bucks for Drone Brains, WIPED (Mar. 29, 2012, 5:13 PM), http://www.wired.com/dangerroom/2012/03/big-data/.

(13.) Chevron Corp. v. Weinberg Grp., 286 F.R.D. 95, 98-99 (D.D.C. 2012).

(14.) PeopleBrowsr, Inc. v. Twitter, Inc., No. C-12-6120 EMC, 2013 WL 843032, at *1 (N.D. Cal. Mar. 6, 2013).

(15.) 132 S. Ct. 945 (2012).

(16.) Id. at 948.

(17.) See id. at 949-50.

(18.) Id. at 964 (Alito, J., concurring).

(19.) See id. at 954-57 (Sotomayor, J., concurring). Perhaps more important, Justice Sotomayor intimated the need to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Id. at 957.

(20.) 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In particular, Justice Harlan, in his concurring opinion, stated: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Id.

(21.) 690 F.3d 772 (6th Cir. 2012).

(22.) See id. at 774-75.

(23.) Id. at 777.

(24.) See id. at 786-88 (Donald, J., concurring).

(25.) See United States v. Jones, 908 F. Supp. 2d 203,206-07 (D.D.C. 2012).

(26.) See id.

(27.) 132 S. Ct. 945 (2012).

(28.) Jones, 908 F. Supp. 2d at 204.

(29.) Id.

(30.) Id.

(31.) Id. at 214 (citing Davis v. United States, 131 S. Ct. 2419, 2427 (2011)).

(32.) See Fair Information Practice Principles, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified Nov. 23, 2012).

(33.) See id.

(34.) See infra Part IV.A.

(35.) See generally Nell M. Richards, The Perils of Social Reading, 101 GEO. L.J. 689, 711-12 (2013) (discussing anonymity as foundational to privacy in the context of social reading).

(36.) See Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data art. 2(a), 1995 O.J. (L 281) 31 (defining "personal data").

(37.) See id. art. 3 (defining the scope of the directive).

(38.) See 42 U.S.C. [section] 1320d-2 (2012) (requiring the Secretary to adopt security standards and safeguards).

(39.) See 45 C.F.R. [section] 164.514(b) (2013).

(40.) See, e.g., Privacy Laws, OFFICE OF THE ATT'Y GEN., STATE OF CAL. DEP'T OF JUSTICE, http://oag.ca.gov/privacy/privacy-laws (last visited Sept. 6, 2013) (collecting California's privacy laws).

(41.) See Larry Hardesty, How Hard Is It to 'De-Anonymize' Cellphone Data?, MIT NEWS OFFICE (Mar. 27, 2013), http://web.mit.edu/newsoffice/2013/de- anonymize_cellphone_data_0327.html.

(42.) See 15 U.S.C. [section][section] 1681-1681x (2012).

(43.) Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), http://www.ftc.gov/opa/2013/05/databroker.shtm.

(44.) Id.

(45.) See Craig Timberg, FTC Warns Data Brokers on Privacy Rules, WASH. POST (May 7, 2013), http://articles.washingtonpost.com/2013-05-07/business/39090758_1_data-brokers- personal-data-data-reports.

(46.) Edward Wyatt, F.T.C. and White House Push for Online Privacy Laws, N.Y. TIMES (May 9, 2012), http://www.nytimes.com/2012/05/10/business/ftc-and-white-house-push-for-online- privacy-laws html?_r=0.

(47.) Press Release, Fed. Trade Comm'n, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 6, 2012), http://www.ftc.gov/opa/2012/06/spokeo.shtm. For more on this and other FTC actions, see Fatima Nadine Kahn, Survey of Recent FTC Privacy Enforcement Actions and Developments, 69 BUS. LAW. 227 (2013).

(48.) See Press Release, Fed. Trade Comm'n, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2012), available at http://www.ftc.gov/opa/2012/03/privacyframework. shtm.

(49.) FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 23-30 (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326 privacyreport.pdf.

(50.) Press Release, Fed. Trade Comm'n, HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers (Feb. 22, 2013), http://www.ftc.gov/opa/2013/02/htc. shtm.

(51.) See id.

(52.) 15 U.S.C. [section] 45 (2012).

(53.) See Press Release, Fed. Trade Comm'n, supra note 50.

(54.) See Jessica Guynn, FTC Calls on Online Ad Industry to Agree on Do-Not- Track Standard, L.A. TIMES (Apr. 17, 2013, 3:41 PM), http://www.latimes.com/business/technology/la- fi-tn-ftc-online-ad-industry-do-not- track-20130417,0,5397711.story.

(55.) See id.

(56.) See H.R. 6377, 112th Cong. [section] 3 (2012).

(57.) See id. [section] 2.

(58.) See id. [section] 4.

(59.) S. 607, 113th Cong. (2013) (reported by Sen. Leahy with an amendment on Apr. 25, 2013); S. 607, 113th Cong. (2013) (originally introduced by Sen. Leahy on Mar. 19, 2013).

(60.) See Press Release, Judiciary Comm., Statement of Judiciary Committee Chairman Bob Goodlatte (Apr. 25, 2013), available at http://judiciary.house.gov/news/2013/04252013.html.

By John Pavolotsky *

* John Pavolotsky, CIPP-US is a technology attorney based in northern California.

Pavolotsky, John

Robots in the Home: What Will We Have Agreed to?

Margot E. Kaminski

Public Law and Legal Theory Working Paper Series
No. 292
Idaho Law Review, 2015 forthcoming

April 20, 2015

This working paper series is co-sponsored by the
Center for Interdisciplinary Law and Policy Studies
at the Moritz College of Law

ROBOTS IN THE HOME: WHAT WILL WE HAVE AGREED TO?

MARGOT E. KAMINSKI*

TABLE OF CONTENTS

I. INTRODUCTION

* Assistant Professor of Law at the Ohio State University Moritz College of Law, and Affiliated Fellow at the Information Society Project at Yale Law School. Thanks to Jack Balkin for co-teaching our Artificial Intelligence and Robots seminar, Ryan Calo for welcoming me into the law-and-robotics community, and Bryan H. Corbellini for giving me a much-needed afternoon off. Thanks also to Amanda Lynch, Scott R. Peppet, and Guy A. Rub for thoughtful comments on an earlier draft.

A new technology can expose the cracks in legal doctrine. Sometimes a technology resists analogy. Sometimes through analogies, it reveals inconsistencies in the law, or basic flaws in framing, or in the fit between different parts of the legal system. This Essay addresses robots in the home, and what they reveal about U.S. privacy law. Household robots might not themselves destroy U.S. privacy law, but they will reveal its inconsistencies, and may show where it is most likely to fracture. Just as drones are serving as a legislative "privacy catalyst"[1]—encouraging the enactment of new privacy laws as people realize they are not legally protected from privacy invasions—household robots may serve as a doctrinal privacy catalyst.

Some household robots are already here: the Roomba already vacuums our floors (and scares our pets). In Japan, and possibly soon in the UK, fuzzy robot seals are used in eldercare.[2] Household and caretaker robots are on the agenda for major technology companies. Bill Gates in 2007 called for a "robot in every home."[3] And Toyota is currently experimenting with "care assist robots" that can lift and carry elderly patients, preventing injury to human caretakers and allowing people with dementia to remain longer in their homes.[4] Mattel has debuted Hello Barbie, a Barbie doll imbued with voice-recognition software.[5] *Robot & Frank*, an only slightly futuristic movie about an elderly man with a friendly caretaker robot, envisions a near future in which privacy, ethics, and relationships are challenged by a helpful household robot.[6]

There are two legal puzzles raised—or revealed—by household robots. First, there is the question of whether a robot's permission to be in a space also grants permission to record information about that space. Second, there is the broader legal question of whether traditional

1. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 (2011).

2. Andrew Griffiths, *How Paro the robot seal is being used to help UK dementia patients*, GUARDIAN (July 8, 2014) *available at* http://www.theguardian.com/society/2014/jul/08/paro-robot-seal-dementia-patients-nhs-japan.

3. Bill Gates, *A Robot in Every Home*, SCI. AM., January 2007, at 58, *available at* http://www.cs.virginia.edu/~robins/A_Robot_in_Every_Home.pdf.

4. Wendy Hall, *Technology could help people with dementia remain in their homes*, GUARDIAN (June 23, 2014) *available at* http://www.theguardian.com/social-care-network/2014/jun/23/technology-help-people-dementia-longitude-prize.

5 http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves/

6. ROBOT & FRANK (Samuel Goldwyn Films 2012).

legal protection of the home as a privileged, private space will withstand invasion by digital technology that has permission to be there. In other words, when we agree to allow robots in our homes, are we correspondingly agreeing to allow them to record? To allow in the third parties with which robots communicate? This Essay's basic claim is that the legal salient aspects of home robots may drive a collision between the legal understanding of privacy in real physical space, and its understanding of privacy in the digital realm. That conflict in turn reveals inconsistent understandings of permission and consent in context, across privacy law.

This Essay begins by identifying the legally salient features of home robots: the aspects of home robots that will likely drive the most interesting legal questions. It then explores how current privacy law governing both law enforcement and private parties addresses a number of questions raised by home robots. First, how does privacy law treat entities that enter places (physically, or through sense-enhancing technology) where they are not invited? Second, how does privacy law treat entities that *are* invited into a physical space, but were not invited to *record* in that space? Third, how does privacy law treat consent, both express and implied? Fourth, how does privacy law address entities that lull—or deceive—people into revealing more than they intend to? And finally, in the private actor context, will robotic recording be considered to be speech?

The rise of robots in the home is a form of technosocial change.[7] Both technology and the social norms around its use will develop—and what is legally salient about home robots is not just a matter of their technological capabilities, but of how we put them to use.[8] That technosocial change will reveal strains in the law's treatment of privacy harms, especially around questions of what constitutes sensitive information, and the role of consent or assumption of risk. Interestingly, evaluating how home robots might be treated under U.S. law reveals that the Fourth Amendment and treatment of private actors are imperfectly aligned in their understanding of privacy.

II. WHY HOUSEHOLD ROBOTS ARE LEGALLY INTERESTING

Robots are embodied technologies that contain software, or code, and move and act on other objects in real space. While there is no single definition of a robot, some consensus has formed around defining

7. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011) (using the term "technosocial" to refer to the "intertwined effects of technological and social change").

8 Jack M. Balkin, *The Path of Robotics Law*, Calif. L. Rev. (forthcoming 2015), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2586570 (pointing out that "As we innovate socially and economically, what appears most salient and important about our technologies may also change.").

robots as technologies that sense, think, and then act on and in the physical world.[9] The Internet of Things and household robots raise privacy questions along the same spectrum, but certain features of robots—that they can move by themselves, may make their "own" decisions, and have social valence—will raise fairly unique privacy questions.

The technical definition of what a robot is differs from what might make a robot interesting from a legal perspective. This Section thus identifies the legally salient aspects of household robots, from the framework of privacy law. To identify the legally salient features of household robots, we must start with an understanding of (1) the privacy harms at issue, and (2) why implied consent or assumption of risk is central to the discussion.

A. Types of Privacy Harm

To understand what aspects of household robots are legally salient, we have to articulate what privacy harms household robots might cause. Robots, as part of their basic functionality, sense and record their environment. They will often share that information with third parties, or store that information in the cloud. Household robots thus pose two basic privacy concerns: concerns over excessive sharing and processing of information, and concerns over initial recording of information.

Information sharing can threaten contextual integrity: the reliance people place on the idea that information revealed in one context will not be moved into or used in another.[10] One type of privacy harm posed by household robots is the breakdown of contextual integrity, when the context in which things are recorded has traditionally been treated as private.[11] When information revealed in the home is shared and used outside of the home, people may stop trusting that the home is a private location, and may conform their behavior to majority norms even

9. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. (forthcoming 2015).

10. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559, 567–68 (1998), *available at* http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf.

11. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

within the home.[12]

A second, related type of privacy harm threatened by household robots has to do with enabling people to manage their social boundaries at the moment at which information is captured.[13] At the moment of an interaction, people use physical features of their environment, such as walls, to manage their social accessibility. They also rely on social relationships—the idea that a trusted person will not disclose information to third parties—and on temporal features of relationships, such as forgetfulness over time. Household robots threaten this "boundary management" because in addition to crossing physical boundaries, or being able to "sense" through physical boundaries using sense-enhancement technologies, their social features may elicit trust where trust is not deserved.

B. Consent or Assumption of Risk

A recurring theme in U.S. privacy doctrine is that in certain contexts, or certain relationships, people assume the risk that information will travel, and thus cannot claim that their privacy has been violated. For example, two people embracing at a fair could not claim that their privacy had been violated when a photograph of the embrace ended up on the front page of a newspaper.[14] And under the Fourth Amendment, you have no reasonable expectation of privacy in the phone numbers you dial, because you share them with the telephone company.[15] Perhaps the biggest doctrinal puzzle raised by household robots will be whether information revealed in a traditionally private location—the home—can be treated as not private because it has been shared with third parties as a necessary part of a robot's functioning.[16]

C. The Legally Salient Aspects of Household Robots

Thus household robots may cause two types of privacy harms: violation of contextual integrity and boundary management challenges. And analysis of whether those privacy harms will be legally protectable may hinge on whether people are understood to be assuming a risk that information will travel, by sharing information with third parties. This understanding gives us the background for identifying the legally salient aspects of household robots.

Ryan Calo has suggested that robots in general will have three

---

12. *See generally* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015).

13. Margot E. Kaminski, *Theory of Privacy for Information-Gathering Laws*, WASH. L. REV. (forthcoming).

14. *See generally* Gill v. Hearst Publ'g Co., 253 P.2d 441 (1953).

15. *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

16 The same conflict with third-party doctrine is raised by the Internet of Things. See Andrew Guthrie Ferguson, The Internet of Things and the Fourth Amendment of Effects, Calif. L. Rev. (forthcoming, 2016) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2577944.

effects on privacy: they will increase the amount of direct surveillance, they will increase access to formerly private spaces, and they will have social meaning.[17] Calo has also suggested more generally that the "essential qualities" of robots—which I understand to be the legally salient qualities of robots—are (1) embodiment, (2) emergence, and (3) social valence.[18] This Essay takes a narrower approach, asking what aspects of household robots in particular are legally salient, from the perspective of privacy law.

The **ability or even need of robots to sense and record information**, and likelihood that they will share that information with third parties sometimes for processing purposes, is clearly a legally salient feature of the technology from a privacy perspective. On the one hand, the fact that robots must take in information to properly navigate an environment (just as a phone call must be made on telephone lines) suggests that the sensing might be treated as necessary for functionality and thus users will remain deserving of legal privacy protection. On the other hand, the known ability of robots to record massive amounts of information about private places raises the question of whether household robot owners have consented to that recording, implicitly or explicitly, by allowing robots into private spaces.

The sensory aspect of robots also raises interesting legal questions about how to treat a robot (1) that records more information than is necessary for functionality; (2) that records more information than it has told its owner it is recording (fails to provide notice); (3) that has been given permission to enter or operate in certain locations, but not to record in those locations; and (4) that senses or records information humans aren't used to monitoring with their own senses (like temperature). Thus the centrality of sensing and recording to household robots' functionality is a legally salient aspect of household robotics, especially when that sensing involves non-visual senses such as thermal imaging.

The **ability of household robots to move** is a second legally salient feature. If a robot can open doors, or go into rooms of a house where it has not been invited, this may indicate that it is capable of violating contextual integrity or threatening boundary management. But if a person fully understands that their household robot is capable

17. M. Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 187–88 (Patrick Lin, Keith Abney & George A. Bekey eds., 2012).

18. Calo, *supra* note 9.

of going wherever it wants, then the known ability of robots to move from room to room or through doors may suggest that the robot's owner has assumed the risk that all areas of the home are no longer private. Thus, movement is one legally salient feature of household robots: depending on how courts characterize it, movement may push the legal doctrine in a number of directions.

The **social valence or social meaning** of home robots—that is, the fact that robots may be anthropomorphic or appear as quasi-human actors—may be salient to privacy law. There is evidence that people treat anthropomorphic robots with increased compassion and trust.[19] A robot that lulls people into revealing more than they intend to may be viewed as deceptive; or treated similarly to false human friends.

Finally, the **ability of robots to process information**, or "think" and "make decisions," may be legally salient. Emergent behavior might affect the scope of implied consent or assumption of risk, if household robots make decisions outside the scope of what their owners believe they have agreed to. If household robots partake in emergent, unpredictable behavior, this may affect discussions of any liability regime for their creators, influencing discussion of whether there should be a strict liability regime or negligence standard, or something else. Should programmers or creators be required to put in safeguards to prevent certain kinds of emergent behavior? Or should they not be held liable for behavior that was truly unpredictable? Finally, emergent behavior will affect legal conversations about the applicability of the emerging First Amendment right to record, and whether robots—or their programmers—should be legally considered to be "authors" of the recorded information they gather.[20]

In summary, the legally salient aspects of household robots include: (1) their need to sense and ability to record vast amounts of information that they likely will share with third parties, who will in turn process that information; (2) their ability to independently move in a physical environment; (3) what Calo calls their "social valence"; and (3) their ability to process information, or "think," in complex, unpredictable ways.

III. WHAT HOUSEHOLD ROBOTS REVEAL ABOUT PRIVACY LAW

This section turns from household robots themselves to what they reveal about U.S. law. New technologies are often incorporated into caselaw by analogy.[21] But trying to fit household robots into existing

19. *Supra* note 9.

20. Jane R. Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 61 (2013); *see also* Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, 5 STAN. TECH. L. REV. 1, 22 (2012) (for discussion of AI authorship in copyright law).

21. Neil M. Richards & William D. Smart, *How Should the Law Think About Robots?* 19 (2013) (prelimary draft), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263363.

boxes under current caselaw reveals problems and inconsistencies in privacy doctrine. This section begins by discussing household robots and the Fourth Amendment, and then turns to law governing private actors.

A. Government and the Fourth Amendment

The home is privileged in Fourth Amendment analysis; it receives paramount privacy protection.[22] The "very core" of the Fourth Amendment is "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[23] In some ways, U.S. privacy jurisprudence treats "information revealed in the home" as its own category of sensitive information.[24]

But the third party doctrine in Fourth Amendment jurisprudence explains that when people voluntarily share information with third parties, they do not have a reasonable expectation of privacy in that information.[25] Other cases similarly suggest that a person has no reasonable expectation of privacy from a privacy-invading technology that is in general or regular public use.[26] Will the centrality of the home in Fourth Amendment jurisprudence withstand the incursion of household robots? The answer to this question depends in large part on the power of analogies, and on how far courts are willing to extend current understandings about assumptions of risk or implied consent to information gathered in the home.

This Section outlines relevant Fourth Amendment caselaw on the following questions: first, how might home robots be treated when they enter or observe physical spaces where they have not been invited? Second, how might home robots be treated when they record information in a location where they have been invited to be—but in which they were not necessarily invited to record? Third, how might the presence of home robots be understood to imply consent to the reuse of information? Fourth, how might actual contractual agreements

22. Kyllo v. United States, 533 U.S. 27, 31 (2001). See also Ferguson, The Internet of Things and the Fourth Amendment of Effects, supra.

23. *Id.* (citing Silverman v. United States, 365 U. S. 505, 511 (1961)).

24. Sensitive information receives more privacy protection. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. (forthcoming 2015).

25. *E.g.*, Smith v. Maryland, 442 U.S. 735 (1979).

26. *See generally* Kyllo v. United States, 533 U.S. 27 (2001); Florida v. Riley, 488 U.S. 445 (1989) (O'Connor, J., concurring) (asking whether "the observation cannot be said to be from a vantage point generally used by the public"); California v. Ciraolo, 476 U.S. 207 (1986)..

and/or privacy policies around home robots be treated, under the Fourth Amendment? And fifth, how might Fourth Amendment doctrine treat falsely reassuring robots?

1. Entering where not invited

Household robots might enter a physical space in a home to which they have not been invited, or use sense-enhancing technology to "see" into that space. The legally salient features of household robots vis a vis this question are their ability to move; to sense using sense-enhancing technology; and possibly the ability to make emergent decisions that cause them to act "independently," contrary to owners' preferences.

Fourth Amendment jurisprudence once was "tied to common-law trespass," although it did not require technical trespass, only "actual intrusion into a constitutionally protected area."[27] The Supreme Court famously decoupled Fourth Amendment violations from trespass in *Katz v. United States*, explaining that the Constitution "protects people, not places."[28] A person's privacy could be protected in an area outside the home and accessible to the public if the person had a reasonable expectation of privacy.[29] But the Supreme Court also observed in *Katz* that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[30]

The question thus is as follows: when a person lets a robot into her house, and assumes it will remain in one area of the house, is it a violation of a reasonable expectation of privacy for the robot whose information is accessed by law enforcement or who has been hacked and is controlled by law enforcement to enter, or use sense-enhancing technology to enter, a room or space where it is not supposed to be?

The Supreme Court addressed a similar question when it evaluated police use of sense-enhancing technology in *Kyllo v. United States*.[31] There, the Court concluded that police could not use thermal imaging to "see" into the interior of the home.[32] The majority analogized thermal imaging to trespass, rather than to naturally emanating information such as smells.[33] The Court explained that "obtaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search at least where (as here) the technology in question is not in general

27. Kyllo, 533 U.S. at 31; Silverman, 365 U.S. at 510–12.

28. Katz v. U.S., 389 U.S. 347, 351 (1967).

29 *See id.*

30. *Id.* at 351.

31. *Supra* note 22..

32 *Id.* at 40.

33. *Id.* at 48.

public use."[34]

The question, then, may be whether police access to information obtained by a robot in searches unauthorized by a homeowner constitutes use of "technology . . . in general public use."[35] Many people may end up with household robots, which may make the robots themselves technology in general public use. But it seems unlikely that people will generally access information from each other's robots, suggesting that government coopting of household robots' ability to move from room to room or see through walls would not reflect technology in general public use.

However, three cases on aircraft photography may cut in the other direction. In *California v. Ciraolo* and *Florida v. Riley*, the Supreme Court found that people do not have a reasonable expectation of privacy with respect to naked-eye observation or aerial photography from a fixed-wing aircraft, or from a helicopter.[36] In a third case, the Court found that enhanced aerial photography did not require a warrant.[37] The Court reasoned in *Riley* that the FAA permits helicopter flight from 400 feet above a home, so people do not have a reasonable expectation that helicopters won't fly and observe them from 400 feet above the home.[38] Justice O'Connor clarified in her concurrence that FAA regulation should matter less than the fact that the use of air travel is such a "sufficiently routine part of modern life" that people no longer have a reasonable expectation of privacy against most aerial surveillance, in the curtilage of their home.[39] These cases suggest that if robots become a regular part of most peoples' lives, courts might not find a reasonable expectation of privacy in information those robots reveal—even if the technology has not been granted express permission to look into particular rooms or spaces.

However, the deciding factor might be the preservationist reasoning relied on by the Court in both *Kyllo* and more recent cases.[40] In a

---

34. *Id.* at 28.

35 *Id.*

36. 476 U.S. 207, 213–14 (1986*);* 488 U.S. 445, 445 (1989).

37. Dow Chemical v. U.S., 476 U.S. 227, 239 (1986).

38 488 U.S. at 445.

39 Id. O'Connor concurrence.

40. *See* Kyllo, 533 U.S. at 27–28; Riley, 488 U.S. at 445; *see also* Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 426, 489–99 (2011).

recent case on searching cellular telephones, and in *Kyllo*, the Court referred to the necessity of preserving the degree of privacy protection in existence at the time the Fourth Amendment was adopted.[41] If this is truly a guiding principle for the Court, then information gathered by nosy, trespassing robots should remain protected by the Fourth Amendment.

2. Recording where they are invited to be, but not to record

A second Fourth Amendment question is how to treat robots that are invited into private spaces, but *not invited to record* or observe using another sense. In other words, people may expect household robots to move around in a space, and perform an expected function, but not to record interactions or share them with other parties over time.

A recent Supreme Court case might be understood as applicable to this scenario. The Court considered whether a drug-sniffing dog brought by police officers onto a porch violated the Fourth Amendment.[42] The Court reasoned that while a police officer may rely on an "implicit license" to walk on the porch to knock at the front door like other visitors, that "implicit license" did not extend to using a trained drug-sniffing dog.[43]

This case suggests that if a household robot has been invited in to a private space, but a person can exhibit a real expectation that the robot would not be permanently recording information or using sense-enhancing technology without notice, that person might have a reasonable expectation of privacy against the unpermitted recording, through whatever sense the robot uses.

3. Implied Assumption of Risk (or Implied Consent)

Both of the previous two scenarios involved a robot breaching its owner's orders. In the above two scenarios, a household robot exceeds explicit permissions (or ignores an explicit ban) by (a) entering (physically or sensually) into spaces unwelcomed, or (b) recording unwelcomed in a space where it physically might be present. But what about when a robot's owner cannot claim to have denied permission to the robot, either to access specific areas or to record the environment? This is where the doctrinal muddle in Fourth Amendment law revealed by household robots—the tension between third party doctrine and protection for the home—gets the most interesting.

Most robots will share information with third parties, for processing purposes or just to store information in the cloud. The Supreme

41. Kyllo, 533 U.S. at 28: "This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"; Riley v. California, 134 S.Ct. 2473, 2494–95 (2014).

42. Florida v. Jardines, 133. S.Ct. 1409 (2013).

43. *Id.* at 1415.

Court has in a line of cases explained that people do not have a reasonable expectation of privacy in information, such as the records of phone numbers dialed, revealed to or stored with third parties.[44] If a person fails to restrict their household robot's access to particular parts of the house, or cannot indicate that she thought the robot wasn't recording, then information gathered by the robot and sent to the cloud or revealed to the robot's seller might fall within third party doctrine. Then police may access that information through the third party, without a warrant. To be clear: there are complex statutory schemes in place for handling police access to stored communications and telephone numbers dialed.[45] But those statutes apply to communications, and thus likely do not apply to most information robots will store.

Justice Sotomayor recently suggested that the third party doctrine has no place in our digital world.[46] And in a recent decision on cell phone searches, Chief Justice Roberts suggested (but did not hold) that people may have an expectation of privacy in phone numbers dialed when that information is combined with more sensitive information.[47] These indicators may suggest that the Court is getting ready to reconsider third party doctrine, or at least considerably narrow its scope. Similarly, a recent D.C. Circuit decision evaluating the constitutionality of the government's bulk storage of telephone metadata (i.e., numbers dialed and more) explained that big data is different in kind from the type of sharing happening when the Supreme Court first created the third party doctrine.[48]

Household robots may place the third party doctrine on even rockier shores. Part of the reasoning in third party doctrine cases is that the information at issue is not particularly sensitive—in the case of phone numbers, it is considered "envelope" information.[49] When household

---

44. Smith v. Maryland, 442 U.S. 735 (1979).

45. *E.g.* Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701 (West 2014); Stored Communications Act, 18 U.S.C. § 2701 (West 2014); Pen Registers and Traps, 18 U.S.C. § 3121 (West 2014).

46. United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).

47. Riley v. California, 134 S.Ct. 2473, 2490 (2014).

48. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); *but see In re* FBI, 2013 WL 5307991 (FISC 2013).

49. Author: Please provide support for this assertion. *But see* U.S. v. Miller, 425 U.S. 435 (1976) on bank records. (But bank records there are possibly treated as "less sensitive" information because perform an act [transaction], not just passive information.)

robots record information in the home, courts may find that home information is inherently more sensitive than "envelope" information like phone numbers, and thus refuse to apply the third party doctrine. We can see this happening in at least two places: first, the Sixth Circuit has held that there is a reasonable expectation of privacy in the content of one's email, even though people technically share their email with third parties such as Google.[50] Second, the Eleventh Circuit has pointed out that location information *in the home* is sensitive information[51]—even though location information outside of the home was held in older Supreme Court cases not to be inherently sensitive information.[52] So there is developing precedent for the idea that being in the home turns information sensitive.[53]

4. Actual (Contractual) Agreements/ Privacy Policies

One of the more interesting questions that might arise around the sharing of information with third parties is the impact of an actual agreement—for example, a privacy policy—on a person's Fourth Amendment "reasonable expectation of privacy." If a person has a robot in their home, and has agreed to a particularly permissive privacy policy, can they still have a reasonable expectation of privacy against the revelation of that information to the government?

The Sixth Circuit addressed this question in its email case.[54] The court reasoned that while some subscriber agreements might be "sweeping enough to defeat a reasonable expectation of privacy… we doubt that will be the case in most situations."[55] Importantly, the Sixth Circuit held that the ability of the third party to access sensitive information—in that case, the contents of emails—does not abolish an expectation of privacy against law enforcement in that information.[56]

5. Lulling people into revealing information

There is no Fourth Amendment doctrine that is clearly analogous to lulling people into revealing information through the social/anthropomorphic features of robots. But what caselaw there is suggests that the Fourth Amendment does not protect us from what we reveal to de-

---

50. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

51. United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) (finding that in light of *Jones*, the Fourth Amendment required a warrant for cell site location information and the Stored Communications Act protections were inadequate). *See also In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010).

52. Author: Please provide support for this assertion.

53. *But see In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

54. Warshak, 631 F.3d at 266.

55. *Id.* at 286.

56. "[T]he mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *Id.*

ceptive or reassuring robots—unless you analogize the robots to diaries rather than people.

One could analogize the idea of the deceptive robot to a "false friend": police do not need a warrant to get information from a confidential informant, or friend who decides to turn on a person.[57] More broadly speaking, the Supreme Court has upheld consent to enter a residence when police commit fraud, or falsely claim to be there for a legitimate purpose.[58] But if robots are instead analogized to diaries or computers, rather than conceptualized as independent actors, then barring third party doctrine and storage of the information elsewhere, there may be a reasonable expectation of privacy in what gets revealed to a reassuring robot-diary.[59] Thus which analogy courts choose may be central to how deceptive robots are treated in the law enforcement context.[60]

B. Private Parties

The government will not be the only party interested in information gathered by household robots. And as evidenced by the above discussion of the third party doctrine, private parties may actually have easier access to information gathered by household robots than law enforcement.

---

57. Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no Fourth Amendment violation where petitioner "was relying upon his misplaced confidence that Partin would not reveal his wrongdoing"); Lewis v. United States, 385 U.S. 206, 212 (1966). The Supreme Court has held that police also do not need a warrant to bug a confidential informant with the informant's permission. United States v. White, 401 U.S. 745 (1971).

58. Lewis v. United States, 385 U.S. 206, 211 (1966) ("A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant."). *See also* United States v. Contreras-Ceballos, 999 F.2d 432, 435 (9th Cir. 1993) ("we have held that a law enforcement officer's use of a ruse to gain admittance does not implicate section 3109 because it entails no breaking"); Dickey v. United States, 332 F.2d 773, 777–78 (9th Cir. 1964); Leahy v. United States, 272 F.2d 487, 489 (9th Cir. 1959).

However, police may not lie about the existence of a search warrant, or lie about their true purpose once they identify themselves as government. *See* Bumper v. North Carolina, 391 U.S. 543 (1968); United States v. Bosse, 898 F.2d 113 (9th Cir. 1990); United States v. Tweel, 550 F.2d 297 (5th Cir. 1977) ("It is a well-established rule that a consent search is unreasonable under the Fourth Amendment if the consent was induced by deceit, trickery or misrepresentation of the Internal Revenue agent."). *But see* United States v. Briley, 726 F.2d 1301 (1984).

59. *See* Riley, *supra* note 47, at 2479 (referring to a diary as a "highly personal item").

60. Neil M. Richards & William D. Smart, *How Should the Law Think About Robots?*, ROBOTS.LAW.MIAMI.EDU (May 2013), http://robots.law.miami.edu/wp-content/uploads/2012/03/RichardsSmart_HowShouldTheLawThink.pdf.

This Section evaluates several questions involving privacy violations by private parties, rather than the government. Most of these overlap with the questions addressed in the context of Fourth Amendment doctrine, above. And interestingly, the answers in the case of private parties may differ. Thus household robots reveal interesting inconsistencies in U.S. privacy law.

This Section first addresses how the law might treat privacy violations by private actors through robots that enter where they are not invited. Then it addresses robots that exceed the scope of their permitted entry into a private space by recording information revealed in that private space. It addresses implied assumptions of privacy risks; and actual contractual agreements. This Section discusses how to address robots that lull people into revealing more information to third parties than they intended, and, finally and briefly, the question of whether household robots' recording of information about their environments could constitute "speech" by private parties.

1. Entering where not invited

In privacy law addressing private actors, as in Fourth Amendment doctrine, trespass and privacy violations can be linked. The Prosser privacy tort of intrusion upon seclusion does not technically hinge on location, but does in practice suggest that there is a reasonable expectation of privacy in privileged solitary places such as the home.[61] If a robot enters a room where it is not invited, acting as an agent of a private party, then it may commit the intrusion tort. Here, a household robot's emergent behavior may create interesting problems with respect to finding liability for those private actors who allegedly control the robot.

California has legislated against the use of new technologies to intrude in areas where entrance would have been trespass, but for the use of the technology.[62] This approach reflects Justice Scalia's language in *Kyllo*, the thermal imaging case, where Justice Scalia noted that virtual entrance into the home by technology not in public use was a Fourth Amendment violation.[63] If a robot is given permission to enter part of the home, but not other parts, it might be in violation of this law in California.

2. Recording where they are invited to be, but not to record

A more interesting question in the case of private actors is whether robots that are invited to be in a location, but not invited to record there, commit a privacy violation. The alternative is that their activity—unlike law enforcement activity—might be protected by the First Amendment. I discuss this prospect more below, in B(6).

---

61. RESTATEMENT (SECOND) OF TORTS § 652(b) (1977).

62. CAL. CIV. CODE § 1708.8(b) (2011).

63 Author: please provide support for this assertion. Probably the *Kyllo* case cite.

Existing case law points in both directions. On the one hand, some courts have found that granting permission to someone to be in a location constitutes granting permission to record, or at least obviates an expectation of privacy.[64] Other courts, however, have distinguished between inviting somebody in or confiding in them, and allowing that person to record that interaction.[65]

In one case, a court held that even though a victim of a car crash understood that a nurse would witness and remember conversations, the crash victim's privacy was violated when those conversations were recorded.[66] In another, reporters who entered a quack "doctor's" home office by pretending to be patients were found by the Ninth Circuit to have violated the quack's privacy, even though they were not technically trespassing.[67] On the other hand, the Seventh Circuit found that news reporters who recorded fraudulent behavior at an eye doctor's office by posing as patients did not violate an expectation of privacy.[68]

Thus the illicitly recording robot may face divided caselaw. The tipping point may be a distinction noted by the Seventh Circuit: unpermitted recording in the home poses a greater privacy risk that unpermitted recording in public.[69]

3. Implied Assumption of Risk (or Implied Consent)

As in Fourth Amendment cases, courts in cases about private actors often find no expectation of privacy where people assume a considerable risk—or implicitly consent—that their actions will not be private. For example, in the case raised earlier in this Essay, when two people embraced at a fair, they were found to have no expectation of privacy that they would not be photographed and put on the cover of a national magazine, because they assumed this risk by appearing together in public.[70] However, a woman photographed with her skirt up

---

[64] Author: please provide support for assertion.

[65] Author: please provide support for assertion.

66. Shulman v. Group W Productions, 955 P.2d 469, 497 (Cal. 1998).

67. Dietemann v. Time Inc., 449 F.2d 245 (9th Cir. 1971). *See also* Food Lion v. ABC Inc., 194 F.3d 505 (4th Cir. 2001) (although that's about First Amendment limits and duty of loyalty, more than privacy.).

68. Desnick v. ABC, Inc., 44 F.3d 1345 (7th Cir. 1995).

69. Pincite Desnick Eye Center. Author: please provide support for this assertion.

70. Gill v. Hearst, 253 P. 2d 441 (Cal. 1953).

at a funhouse ride was not found to have assumed the risk of this incident occurring, even though it took place in public, likely because her exposed body fell into the category of sensitive information.[71]

Assessment of whether owning a household robot implies consent to having information recorded may once again hinge on whether courts treat information revealed in the home as sensitive, or break it into subcategories where some information is not sensitive and some (for example, sexual or bodily information) is.

4. Actual (Contractual) Agreements/Privacy Policies

The most interesting area of privacy law governing private actors with respect to household robots—and the area revealed to be most different from Fourth Amendment caselaw—involves actual contracts or privacy policies. Remember, in the Fourth Amendment context courts have applied the third party doctrine to find that people usually do not have an expectation of privacy in information revealed to third parties, hinging in part on the consent.[72] But in the private actor context, courts sometimes find expectations of privacy even when a person has technically consented to share that information with others.[73] And the FTC's enforcement capabilities are built precisely around the notion that one has an agreement in place with a third party.

Privacy policies in general are not treated as enforceable contracts.[74] Christine Jolls has noted that in some contexts, courts outright ignore written agreements in cases evaluating privacy violations.[75] Courts look beyond consent, even when it is given by written agreement, to substantive privacy norms.[76] Similarly, the Federal Trade Commission (FTC) uses its Section 5 authority to enforce against private companies not only when they fail to uphold their own privacy policies, but also when a privacy policy is found to be inadequate, or "unfair."[77]

In other words, in the Fourth Amendment context, courts use actual or implied consent to explain away a privacy interest, where in the private actor context, they are more inclined to consider substantive privacy norms even where consent has technically been granted.[78]

A company drafting privacy policies for household robots may

---

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

72 Author: Please provide support for this assertion.

73. Christine Jolls, *Rationality and Consent in Privacy Law*, [insert journal when we figure it out] (forthcoming [insert date]).

74 See e.g. Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004); In re Jet Blue Airways Corp., Privacy Litigation, 379 F. Supp. 2d 299 (E.D. N.Y. 2005).

75 Author: Please provide support for this assertion.

76. *See generally* Jolls, *supra* note 73.

77. Woodrow Hartzog & Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

78 Author: Please provide support for this assertion.

thus wish to strongly consider whether the policy adequately encompasses both industry standards and general privacy norms. As a practical matter robots may be particularly ill equipped to fit with the current notice-and-choice privacy regime, when they lack input and output capabilities or are designed (for deliberate or other reasons) to calm consumers into accepting their activity.[79]

5. Lull into revealing more than intend to

The reassuring or lying robot may receive harsh treatment from privacy law governing private actors. The treatment of deceptive private actors varies even more noticeably from the Fourth Amendment's permissive treatment of "false friends" and lying law enforcement. Remember, when reporters lied and said they were patients to gain access to a quack "doctor's" home office, they were found to violate his privacy.[80]

The FTC also enforces against deceptive actors, who lie to get private information.[81] The FTC also, fascinatingly, enforces against actors that use *technological design* to elicit information, or to falsely indicate that something is private when it is not.[82] The line of FTC enforcement against deceptive or unfair technological design seems directly applicable to the anthropomorphic design characteristics of robots. If a robot appears trustworthy where it is not, it may be deemed deceptive by the FTC.

6. Is recording Speech (and whose)?

A final but very important issue with respect to the use of robots by private actors involves line of developing First Amendment doctrine. A number of courts of appeals have recognized some version of a First Amendment "right to record," often in the context of citizens

79. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 140–41 (2014) (explaining with respect to the Internet of Things that "[t]he basic mechanism of notice and choice—to display and seek agreement to a privacy policy—can therefore be awkward in this context because the devices in question do not facilitate consent.").

80. Dietemann, 449 F.2d at 245; *but see* Desnick, 44 F.3d at 1345. .

81. *E.g.*, Press Release, Federal Trade Commission, Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos (Jan. 29, 2015) *available at* https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges.

82. Hartzog, Solove FTC pincite. Author: Please provide support for this assertion.

using their cellular telephones to record police officers.[83] A private company in Utah used this "right to record" to challenge Utah's law governing information-gathering by automated license plate readers.[84] Utah amended the law so that it now applies only to law enforcement, and not private actors.

There is a real question of whether household robots—or really, the private parties that built them or correspond with them—have a First Amendment "right to record" in private spaces. Most interactions will be governed by voluntary privacy policies that can be enforced by the FTC. But in instances where states wish to create new privacy laws, they may have to keep the First Amendment in mind. Once again, however, the fact that this information is being revealed and recorded in the home may outweigh any interest in "newsworthy" information that might be revealed, under First Amendment newsgathering doctrine. In light of Supreme Court case law rejecting distinctions between high value and low value speech, however, this argument might struggle in courts.

Moreover, there is a legitimate question of whether robots or the private parties that programmed them constitute "speakers" at all.[85] Here, again, emergent behavior makes for an interesting conversation. How directly involved in recording decisions do private actors have to be, to garner First Amendment protection? If a private actor decides to "record all," will that gain more or less protection than one who gives a robot the ability to make its own decisions about what to record?

IV. CONCLUSION AND SUMMARY OF WHAT HOME ROBOTS REVEAL

In conclusion, household robots reveal a number of interesting tensions in U.S. privacy law. Those tensions currently exist, but the introduction of a new technology into the privileged private space of the household may bring these tensions to a head. Household robots, in other words, may be a doctrinal privacy catalyst.

Doctrinally, household robots will require courts to further consider the relationship between privacy, permission, and trespass. Courts will have to decide whether granting permission to an entity to be in a place also grants them permission to record information about that space. Courts will have to reconsider whether information can be private vis a vis a larger audience, even if one agrees to share it with a much smaller audience. Courts will also, in the Fourth Amendment context, have to reconcile treatment of the home as deserving of the

---

83. *See* ACLU v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012) *cert. denied*, 133 S. Ct. 651 (2012); Glik v. Cunniffe, 655 F.3d 78 (1st Cir. 2011); Smith v. City of Cumming, 212 F.3d 1332 (11th Cir. 2000); Kelly v. Borough of Carlisle, 622 F.3d 248, 262 (3d Cir. 2010).

84. Author: Please provide support for this assertion.

85. *See generally* Stuart M. Benjamin, *Algorithms and Speech*, 161 U. PA. L REV. 1445-1493 (2013); Oren Bracha, *The Folklore of Informationalism: The Case of Search Engine Speech*, 82 FORDHAM L. REV. 1629 (2014); James Grimmelmann, Speech Engines, 98 Minn. L. Rev. 868 (2014).

utmost privacy protection with the third party doctrine.

Additionally, considering household robots reveals two interesting substantive splits between the Fourth Amendment approach to privacy, and the approach we use to address private actors. First, the Fourth Amendment tends to take a broad view of consent as obviating a privacy interest, while law governing private actors is sometimes more skeptical and looks to substantive privacy norms.[86] Second, and related, Fourth Amendment doctrine is more permissive of lying to get information, while law governing private actors allows for enforcement against deception—even deception by technological design.[87]

But perhaps what household robots most reveal is the continued need in the United States for a holistic approach to big data. Currently, U.S. privacy law is a patchwork of sectoral federal laws, in contrast with the EU's holistic approach to data privacy. To address real problems of unfairness and violations of contextual integrity using data gathered by household robots, we may wish to use household robots to enact data privacy laws, based on Fair Information Practices that require notice, consent, access, amendment, use limitations, purpose specifications, data accuracy, and data security safeguards.[88] The United States currently places much reliance on standards set by private parties and enforceable by the FTC.[89] But perhaps the advent of household robots will finally bring (truly) home the notion that data processing carries with it real privacy and unfairness risks—and force legislators to address issues raised by information practices. Otherwise, Bill Gates's hope of a robot in every home may go unrealized, and many robots may—after a few prominent privacy violations— be left at the front door.

---

[86] Author: Please provide support for this assertion.

[87] Author: Please provide support for this assertion.

[88] OECD cite

89. *E.g.*, NTIA process