RE-CONCEPTUALIZING PRIVACY LAW IN THE AGE OF DRONES, TWITTER, AND TERRORISM: THE COMING DEMISE OF *KATZ* AND THE REBIRTH OF PRIVACY IN THE 21ST CENTURY

STUDENT SCHOLARSHIP WORKSHOP SERIES

DUKE UNIVERSITY SCHOOL OF LAW

BY: ANDREW K. GERSHENFELD [†]

J.D. CANDIDATE CLASS OF 2017

[†] Duke University School of Law, J.D. expected 2017; Duke University Divinity School M.T.S. 2014; Pennsylvania State University, B.S. 2010.

TABLES OF CONTENTS

ABSTRACT

In this paper I will argue that drones are primed to collide with current Fourth Amendment jurisprudence. In precipitating the current framework' decisive demise, I predict drones will also bring about a veritable privacy revolution that will renew the court's institutional vitality and the Fourth Amendment's enduring legitimacy.

This privacy renaissance will likely occur in one of three ways. First, if the logic underlying the special needs and foreign intelligence exceptions are expanded to include a new "National Security Exception" to accommodate the extraordinary intelligence capabilities of drones—these so-called "exceptions" will soon produce authorized warrantless surveillance so expansive, so pervasive, and so far-reaching as to virtually render the assurances of Fourth Amendment non-existent and eviscerate the substantive distinction between foreign and domestic intelligence surveillance altogether. Second, if domestic drone surveillance is permitted under conditions requiring a lesser standard than probable cause, Fourth Amendment constraints will be relegated to a largely irrelevant status on the basis of their inability to provide meaningful privacy protection precisely when it is needed most. In either of these two circumstances, it appears that big changes in privacy law are on the horizon—as drones will either erode Fourth Amendment protections from within or taking a wrecking ball to them from without. Yet still a third possibility remains, in which Katz collapses under the sheer weight of its own outmoded assumptions, self-defeating circularity, and brazen violation of our most foundational principle of Constitutional law—namely that when weighty matters of fundamental rights are at stake—the tyranny of public opinion simply has no place. Accordingly, if any of these three events obtain, Katz will fall and a new privacy framework will rise to take its place.

Secondly, building on that critique and prediction, I will argue just as Katz reasonable expectation test essentially replaced the outdated trespass framework of Olmstead—so too a use-based, mosaic theory of privacy must in due time replace Katz increasingly antiquated framework as well. As each successive generation slowly, but surely acclimates to greater erosions in their individual and collective expectations of privacy—Katz' "reasonable expectation" test may soon be forced into an early retirement along with other soon to be antiquated theories like the "open field doctrine," "knowing-exposure" doctrine and "third party doctrine"—as relics of a bygone era having outlived their usefulness and overstayed their welcome in an age where social networks inform our norms, Moore's Law dictates the pace of change, and drones will soon rule the domestic skies.

Thirdly, I contend that a use-based, mosaic theory of privacy will be far more apt to produce legal rulings that are amenable to empirical evaluation and critique, more inclined to achieve optimal levels of security, ameliorate law enforcement efficiency and effectiveness, significantly reduce the number of invasive governmental intrusions into our daily lives, and ultimately renew the spirit of America as a nation deeply and profoundly committed to protecting the principles of privacy and autonomy embodied in our Fourth Amendment.

Finally, I argue that a system of shared responsibility between the Federal government and the States will prove crucial to ensure that drones usage by law enforcement and intelligence officials remains consistent with our nations values and our Constitutional principles. This will require a great deal of democratic deliberation and discernment and ultimately beg the larger question of privacy's raison de'etre—what makes freedom worth having, our lives worth living, and our laws capable of enduring.

INTRODUCTION

A. The Future of Drones in America

Unmanned aerial vehicles, popularly known as "drones," will soon rule the domestic skies[1] as we enter into a new chapter in American history—*the age of drones*.[2] This revelation has been received as a promising and welcomed development by many in government, yet many civilians find the prospect of domestic drones highly alarming, and particularly perilous for a nation that has long prided itself on the values of privacy and individual autonomy. As, one commentator has succinctly described this strange amalgam of emotional responses: "drones represent a singular inflection point of fear, of paranoia, of wonder, of technological wizardry, and [of unfettered] future possibility."[3]

Given this unique blend of concern, fear, and wonderment at the future possibilities in store, the precise contours of this new age we are now entering still remain very much open textured questions, to be answered by the leaders of this generation. The stakes are very high and the margin of error is very slim as the answer we give—or *fail* to give—will likely determine the

[1] According to the FAA "30,000 drone aircrafts" are expected to patrol the nation's skies by the year 2020. Shaun Waterman, *Drones over U.S. get OK by Congress*, (Feb 7, 2012) http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/?page=all

[2] Throughout this paper I will refer to unmanned aerial vehicles (UAVs) as "drones" for several reasons. First, for the sake of clarity since it is generally referenced by the public in this manner. Secondly, for the sake of simplicity since the terminology has gone through several iterations ranging from "unmanned aircraft" to "remotely piloted aircraft" to "unmanned aerial vehicles" (UAV) which have all been subsequently abandoned in lieu of the new terminology "Unmanned Aerial Systems" making these various distinctions needlessly complex, overly technical, and gratuitously nebulous for the general reader. Third and most importantly, the new terminology "UAS" functions like a sterile, lifeless term *obscuring* rather than *capturing*—as the evocative imagery conjured up by the term" drone" so aptly does—the public's justified fear, angst, and deep-seated suspicion towards this new technology.

See also ADAM ROTHSTEIN, DRONE, 135-136 (2015) (explaining the importance of the terminology battle between the public and various military-industrial enterprises and what it reveals about society)("The military and commercial drones Company shy away from the term 'drone' preferring a number of acronyms without the heavy narrative of the drone as 'Unmanned Aerial Systems' (UAS) 'Unmanned Vehicle' (UV) 'Remotely Piloted Vehicle' (RPV) and other alphabet soup designations so common the military industrial complex … Despite the attempts of the military to rebrand the drone as simply another technological system the name "drone" has stuck. This singular name works for society at large … *No other word would suffice at this point in history*") (emphasis added).

[3] ADAM ROTHSTEIN, DRONE, 135-136 (2015).

effectiveness of our National security, the boundaries of our civil liberties, the vitality of our values and way of life, and ultimately define the character of our nation.

These far-reaching implications are simultaneously driven and amplified by the unprecedented capabilities of drone technology. Thus, in order to more fully appreciate just how remarkable and extraordinary the challenges posed by drone technology will be it will prove instructive to begin by examining a series of hypotheticals that will illuminate the long and daunting regulatory and jurisprudential road ahead.

In our first hypothetical situation, consider the following scenario: a fifty-five pound government drone is flying overhead a small city and conducting a search-and-rescue mission. As the drone is flying overhead it happens to observe a woman being assaulted and then murdered in plain view of the drone's surveillance camera. Under our future legal regime would privacy purist prefer the drone discard this information since it is not germane to the target search and rescue mission or alternatively would our collective sense of outrage at the perpetration of this heinous crime dictate that the evidence against this individual not be withheld as a matter of justice?

Consider a second scenario. This time, the drone is conducting the same search and rescue mission mentioned in the previous example, but now the drone happens to stumble upon John Doe sliding into second base during a charity softball game. The only problem is that John has stated on his insurance claims that he is unable to return to work due to extensive injuries and the facial recognition technology on the drone has verified his identity, calculated his speed of movement from first to second base, and promptly notified officials of his potential health insurance fraud. Should the software auto-erase his detection or would the aggregate benefit to

society of potentially lower health insurance premiums resulting from increased detection and deterrence of fraud justify exposing John's fraudulent claims?

Third and finally, consider the same hypothetical search mission as above, but this time the drone happens to detect Jane Doe driving over the speed limit, failing to come to a complete stop at a stop sign, and jaywalking thereafter. The drones state-of-the-art license-plate detection technology software identifies her vehicle in the DMV registry, flags the three violations, and automatically mails three tickets to Jane's permanent address on file. Has the government gone too far or merely tapped into its latent potential for full and vigorous enforcement of the laws?

As I hope these illustrative examples indicate, many new legal and ethical issues will emerge as drones enter our domestic skies. In fact, the prospect of near perfect enforcement of the laws will soon be within our grasp as the cost of surveillance will fall precipitously and ability to detect violations will increase dramatically. Consequently, the information that is collected and what we as a society permit to to be used by law enforcement officials will have profound implications for shaping our collective norms and defining the manner in which we lead our everyday lives.

B. A Privacy Renaissance?: Drones, Technological Innovation, and The Need for New Conceptual Wineskins

Like death and taxes, law it is said invariable lags behind technology.[4] The familiar narrative typically proceeds in this manner: as technology evolves lawmakers and courts struggle to keep pace.[5] Legal literature abounds with this familiar motif, "The hare of science and technology lurches ahead. The tortoise of the law ambles slowly behind."[6] Reality may be a bit

[4] Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep up with Technological Change*, Univ. Illinois J. L., Tech. & Pol'y, Issue 2, 239 (Fall 2007).

[5] *Id.*

[6] John H. Pearson, *Regulation in the Face of Technological Advance: Who Makes These Calls Anyway?,* 13 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1, 1 (1999)

more complex, however, when one considers—not merely change in the abstract—but radical change in its concrete reality. That is to say, under certain circumstances a particular technology may present changes that so drastic and its impact on our lives so profound that it forces us to re-think and perhaps even *re-imagine* the very purpose and trajectory of that area of law altogether. The ensuing result is thus no mere *update* in the existing law, but instead a *transformation* and paradigm-shift in the very substance and essence of the law itself.

One such example took place when the revered Roman property doctrine of "*cujus est solum ejus est usque ad coelom*" was swiftly and surprisingly upended in the 20th century with the advent of the airplane and commercial flight. As Justice Douglas explained in *Causby*:

> It is [indeed] ancient doctrine that at common law ownership of the land extended to the periphery of the universe … *but that doctrine has no place in the modern world*. The air is a public highway, as Congress has declared. Were that not true, every transcontinental flight would subject the operator to countless trespass suits. Common sense revolts [that] idea. To recognize such private claims to the airspace would clog these highways, seriously interfere with their control and development in the public interest, and transfer into private ownership that to which only the public has a just claim."[7]

Accordingly, the once revered doctrine was decisively relegated to the trash heap of history as a direct consequence of its inability to accommodate the novel realities of the new age of flight. As this brief example indicates, the *kind* of the change—not just the pace of change itself may have a profound impact on the continuing viability of existing legal doctrines. When such a radical change presents itself, tame and mild responses tinkering within the bounds of existing law may not suffice. As *Causby* amply illustrates, even millennia of settled doctrine are no match for the march of technology and its sweeping, paradigm-shifting potential.

Drones, I contend, will introduce precisely this sort of radical, disruptive energy into our current Fourth Amendment jurisprudence and usher in a veritable privacy renaissance. That is to

[7] 328 U.S. 256, 260-61 (1946).

say, drones will provide "just the visceral jolt"[8] we need—to stop pouring new wine into old wineskins[9] and start thinking afresh and anew about the interplay between privacy, security, and technology in the 21st century.

The exact nature of this transformation will depend in large part upon the surveillance capabilities that drones develop (**Part I**), the restrictions imposed by Federal and State regulations (**Part II**), and the privacy floor[10] set by the Supreme Court (**Part III**). After examining each of these respective issues we will conclude with an Evaluative Synthesis that will offer regulatory prescriptions for Federal and State lawmakers (**Part IV**) along with a proposed jurisprudential paradigm shift (**Part V**) away from the outmoded assumptions and self-defeating circularity of *Katz* towards a fresh, new used-based, mosaic theory of privacy fit for this extraordinary times in which we live.

I.
DRONE TECHNOLOGY:
AN ASSESSMENT OF CURRENT CAPABILITIES AND FUTURE DEVELOPMENTS

The proliferation of small unmanned aerial systems in the U.S. is coming. But are we ready to deal with the threats that could come with this emerging technology? –Scott Perry[11]

---

[8] M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE (2011), http://www.stanfordlawreview.org/online/drone-privacy-catalyst. (explaining how drones may catalyze updates in privacy law) ("Drones and other robots have the potential to restore that mental model. They represent the cold, technological embodiment of observation. Unlike, say, NSA network surveillance or commercial data brokerage, government or industry surveillance of the populace with drones would be visible and highly salient. People would *feel* observed, regardless of how or whether the information was actually used. The resulting backlash could force us to reexamine not merely the use of drones to observe, but the doctrines that today permit this use.") Id.

[9] Matthew 9:17 (King James) ("Neither do men put new wine into old bottles: else the bottles break, and the wine runneth out … but they put new wine into new bottles, and both are preserved.").

[10] In stating that the Fourth Amendment could be construed as a floor I seek to emphasize the fact that Congress and the President are free to institute "more stringent restrictions" than the Courts, if they so desire. Richard M. Thompson, Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses, 2 (April 3, 2013). See id. at 2 (explaining how Miller effectively overturned the Court's decision to not protect information voluntarily provided to banks, by enacting the Right to Financial Privacy Act, P.L. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §3401-3422), which created new statutory protections for bank records.) Consequently, the Court's jurisprudence *sets the floor*, while leaving ample room for the respective States and for Congress to determine the appropriate ceiling.

[11] Scott Perry, Opening Statement of Subcommittee Chairman Scott Perry (R-PA) Subcommittee on Oversight and Management Efficiency "Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies", March 18 2013 (available at https://homeland.house.gov/files/documents/3-18-15-Perry-Open.pdf).

Drones come in a wide variety of shapes and sizes and equipped with a dizzying array of auxiliary accessories. With all their variation, however, drones can be succinctly categorized into one of two main groups: the first possesses what is called "wide-area persistent surveillance" capabilities ("WAPS") and the second group does not ("non-WAPS"). The distinguishing feature of a wide-area persistent surveillance systems like the Department of Defense's ARGUS-IS is that it is capable of monitoring very large areas for an extended period of time—hence the name *wide-area*, *persistent* surveillance—and can be mounted on either manned or unmanned platforms.[12] Conversely, drones without these WAPS capabilities are much less threatening to the general public since they are not capable of tracking individuals' movements over time in the absence of literally following them around from place to place. Accordingly, a brief case study of the ARGUS-IS will amply illustrate these differentiated capabilities and highlight the considerable regulatory and jurisprudential challenges they pose.

A. Case Study: The Future of Drones equipped with ARGUS-IV Technology

The ARGUS-IS[13] is truly a surveillance system without peer—an all-seeing eye in the sky that makes Jeremy Bentham's famed "panopticon"[14] appear utter trivial and insignificant by comparison. Created by the Department of Defense for military purposes, it is a marvel of technological wizardry and engineering mastery. It is the functional equivalent of a legion of

[12] Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), *ARGUS-IS Delivers Unprecedented Situational Awareness Using Onboard, Embedded Image Processing Algorithms*, http://www.baesystems.com/en-us/product/autonomous-realtime-ground-ubiquitous-surveillance-imaging-system-argusis.

[13] Stands for "Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System." *Id.*

[14] JEREMY BENTHAM, THE WORKS OF JEREMY BENTHAM: PANOPTICON, CONSTITUTION, COLONIES, CODIFICATION (Volume IV: 1843).

Predator drones working in unison to survey an area approximately 36 square miles in diameter, or a city the size of Manhattan.[15]

Its surveillance capabilities are so impressive, no object that moves is able to escape or evade its extraordinary tracking capabilities.[16] In fact, by ingeniously aggregating 368 imaging chips to form a composite focal plane array (CFPA)[17]—the ARGUS' mosaic imagery has a resolution so powerful and precise that it can produce a stunning "1.8-billion-pixel" video stream depicting objects as "small as six inches" in diameter from a staggering 20,000 feet away.[18]

Equally astonishing is its considerable memory storage capacity. ARGUS-IS is capable storing absolutely everything it captures up to "a million terabytes of video a day" which amounts to a storage capacity of approximately "5,000 hours of high-definition footage."[19] In effect this allows its operators to be omniscient with respect to the public events taking place in the area beneath the WAPS system, which is why some have called this technology a "time machine for police."[20] The name is justified since operators can view any event in the past with perfect precision.[21] As its creator Dr. John Antoniades explained, operators can simply say, "I would like to see what happened at this particular location three days, two hours, four minutes

[15] *Rise of the Drones: Meet a new breed of flying robots, from tiny swarming vehicles to giant unmanned planes.*, PBS (Jan 23, 2013), http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html

[16] *Id.*

[17] Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), *ARGUS-IS Delivers Unprecedented Situational Awareness Using Onboard, Embedded Image Processing Algorithms*, http://www.baesystems.com/en-us/product/autonomous-realtime-ground-ubiquitous-surveillance-imaging-system-argusis.

[18] *Id. See also, DARPA's 1.8 gigapixel cam touts surveillance from 20,000 feet*

[19] *Id.*

[20] Craig Timberg, *New Surveillance Technology Can Track Everyone In An Area For Several Hours At A Time*, WASHINGTON POST (Feb 14, 2014). https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html

[21] Simply by "reach[ing] back into the forensic archive," it can "create video windows," "detect and track moving vehicles," and even "generate 3D models" just for good measure. BAE Systems, *Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS)*, http://www.baesystems.com/en-us/product/autonomous-realtime-ground-ubiquitous-surveillance-imaging-system-argusis

ago" and ARGUS-IS would actually stream that information on the screen as if it were happening live.[22]

In the near future, the ARGUS surveillance system will be mounted on "a long-range platform like the giant Global Hawk or the Solar Eagle" and remain aloft for months or years at a time.[23] Needless to say, with a surveillance system as powerful as the ARGUS-IS—capable of viewing a city the size of Manhattan, displaying images in high-definition within six inches of focus and storing unlimited information for days at a time—the promise and peril of wide-area persistent-surveillance systems are quite unlike anything we have ever encountered before.

B. Overview of Non-WAPS Drone Surveillance Technology: General Capabilities and Uses

As the above ARGUS-IS case study highlights, drone capabilities are advancing at a rapid pace and the potential uses for law enforcement and intelligence officials are expanding by the day. It should be noted, however, that although the ARGUS-IS is undoubtedly the wave of the future and perhaps the most formidable and impressive airborne surveillance system to date—drones used by law enforcement officials are not likely to be uniform. Instead they will likely vary a great deal depending on the context in which they are employed and objective for which they are are deployed.

1. Size

Depending on the circumstance, some drones may be as small as an insect, yet others may be as large as a commercial airliner.[24] The largest drone currently in use is the Israeli-made Eitan, which is about the equivalent size of a Boeing 737 jetliner.[25] The Eitan has a wingspan of

[22] *Id.*
[23] *Id.*
[24] Jeremiah Gertler, U.S. Unmanned Aerial Systems, CRS Report R42136, 2 (January 3, 2012) https://www.fas.org/sgp/crs/natsec/R42136.pdf (emphasis added)
[25] American Civil Liberties Union, Brief submitted to the Senate Jud. Comm. hearing on "The Future of Drones in America: Law Enforcement and Privacy Considerations," 2 (Mar. 20, 2013), http://www.judiciary.senate.gov/imo/media/doc/CHRG-113shrg81775.pdf.

about 86 feet, an airborne capability of approximately 20 hours, and can reach a maximum altitude of around 40,000 feet.[26] Similarly, the Predator B drone has a wingspan of around 66 feet, an airborne capability of approximately 30 hours, and can reach a maximum altitude of around 50,000 feet.[27] Smaller drones than these, however, appear to be "the current favorite for domestic deployment" by government officials.[28]

Many more variations are still in development too. The aforementioned SolarEagle, is projected to have a wingspan of approximately 120 meters and will utilize "solar energy" as its power source to remain aloft for potentially months or years at a time.[29] Additionally, the developmental RoboBee will have a wingspan of approximately three centimeters, weigh just eighty milligrams, and be propelled "by two insect-like wings that flap 120 times per second."[30] Lastly, the Nano Hummingbird, will weigh in at just 19 grams, and prove particularly useful for missions requiring stealth surveillance as it can nimbly maneuver in small spaces and run on a single AA battery.[31] As this brief survey suggests, the shape or form that a given drone may take may be limited only by the boundaries of our imagination.

2. Equipment

The equipment drones carry will also have a crucial impact on our privacy and security as well. Many drones will carry high-powered zoom lenses capable of providing high resolution video, infrared and ultraviolet night vision, and radar technology that can see through walls and

---

, at 60 (citing "Israel unveils world's largest UAV," Homeland Security Newswire, (Feb. 23, 2010), http://homelandsecuritynewswire,cornlisrael-unveils-worlds-largest-uav.)

[26] *Id.* at 60 (citing R.P.G. COLLINSON, INTRODUCTION TO AVIONIC SYSTEMS, 495 (2011)).

[27] *Id.*

[28] ACLU, *supra* note, at 2.

[29] *Id.* Matthew R. Koerner. *Drones and the Fourth Amendment*, 64 Duke L. J. 1129, 1161 (2015).

[30] *Id.*

[31] ACLU, *supra* note 25, at 62.

even track individuals inside buildings.[32] Many drones will likewise come equipped with "automated license plate readers" to track automobiles as well as "facial recognition technology" to track suspects movement patterns.[33] Additionally, "sense-enhancing technology" may be included as well replete with audio recorders and "sniffers" capable of detecting "biological, chemical, radioactive, or explosive agents."[34] Similarly, in the near future drones will be outfitted with "biometric recognition" technology which will "recognize and track individuals based on attributes such as height, age, gender, and skin color."[35] Lastly, synthetic-aperture radar technology will soon provide government officials with the ability to "identify footprints and tire tracks" as well.[36]

3. Future Possibilities: Autonomous Flight, Artificial Intelligence, and Integrated Informational Systems

Surprisingly, human pilots may no longer even be necessary either. It is quite remarkable that several drone models can "already fly autonomously" without any assistance from human pilots whatsoever.[37] Although most drones do not yet possess this capability, most can, however,

[32] As the ACLU has noted, "A technology called Synthetic Aperture Radar … can see through cloudy and dusty conditions and through foliage, and has the potential to penetrate the earth and walls." *Id.* at 62 (citing Alicia Tejada, *MIT Develops New Radar Technology: Military Could See Through Walls*, ABC News, (Oct. 20, 2011), http://abcnews.go.com/Technology/radar-technology-mit-waIIs/story?id= 14773871).

[33] Richard M. Thompson II, *Domestic Drones and Privacy: A Primer*, CRS Report R43965, 3 (March 30, 2015) http://fas.org/sgp/crs/misc/R43965.pdf.

[34] Matthew R. Koerner Drones and the Fourth Amendment, , 64 Duke L. J. 1129, 1152 (2015). (citing 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.)

[35] Richard M. Thompson II, Domestic Drones and Privacy: A Primer, CRS Report R43965, 3 (March 30, 2015) http://fas.org/sgp/crs/misc/R43965.pdf.

[36] David L. Weiden, *Drones, Domestic Survillance, and Privacy: Legal and Statutory Implications*, in in PRIVACY IN THE DIGITAL AGE, 245 (eds. NANCY S. LIND & ERIK RANKIN 2015).

[37] Koerner, *supra* note 34, at 1152 (citing STEVEN J. ZALOGA, UNMANNED AERIAL VEHICLES: ROBOTIC AIR WARFARE 1917–2007, at 2 (2008).

be controlled through devices as ubiquitous a "smartphone, tablet or laptop computer" and provide streaming video directly back to that device.[38]

In the years to come, drones are also likely to become increasingly "smart." In fact, Korean researchers are currently in the process of experimenting with artificial intelligence to assist robots in learning how to "hide from and sneak up on a subject."[39] Additionally, since many of these models do not make much noise and in some cases do not fly at all—like the "snake bot"[40]—many drones will soon be able to spy surreptitiously on unsuspecting parties with the swiftness and finality of "a thief in the night."[41]

Drones will also soon be able to be integrated with other networks of information to provide a consolidated portrait of one's life—from an individual's employment history, to criminal background, to even one's health history.[42] As one scholar has noted facial recognition technology may soon hold the potential to connect the proverbial dots between one's public life and one's private online transactions by permitting government to consolidate these previously "separate worlds."[43]

4. Practical Effects: Cost-Efficiency and Removal of Traditional Surveillance Barriers

Finally, the costs of drones bears noting with equal emphasis as their functional capabilities. All these incredible features come at a cost that is considerably less expensive then the traditional alternative—*manned* aerial surveillance. Consequently, since drones are "cheaper

---

[38] Jennifer O'Brien, *Warrantless Government Drone Surveillance: A Challenge to the Fourth Amendment*, 30 JOHN MARSHALL J. INFO. TECH. & PRIVACY L. 155, 162 (2013).

[39] ACLU, *supra* note 25, at 61. (citing M. Ryan Calo, "Robots and Privacy," April 2010, online at http://ssm.com!abstract~1599189).

[40] Leo Kelion, *Snake Robots Team Up With Search-And-Rescue Dog In US*, BBC News, (April 29, 2013), http://www.bbc.com/news/technology-22340218.

[41] Weiden, *supra* note 25, at 245; Senator Lee, *The Future of Drones In America: Law Enforcement and Privacy Considerations*: Hearing Before the S. Comm. on the Judiciary, 113th Cong., 1, 17 (2013) http://www.judiciary.senate.gov/imo/media/doc/CHRG-113shrg81775.pdf.

[42] Stepanovich, *supra* note 41, at 32.

[43] Stepanovich, *supra* note 41, at 32.

to fly, cheaper to buy, [and] cheaper to maintain" more governmental surveillance is likely to result.[44] Additionally, since manned aircrafts have always been expensive "to purchase, operate and maintain" resource-bound institutions have traditionally been confined by "natural limits" on the their ability to conduct aerial surveillance operations.[45] Freed from these logistical and financial restraints, however, drones will present considerable privacy and security challenges for Congress and the Courts to control.[46] As this drone technology continues to advance many federal, state and local lawmakers are increasingly taking note and moving into action.

II.
STATUTORY FRAMEWORK: STATE AND FEDERAL REGULATIONS

This is a whole new world now and it has many complications … how does it all get sorted out? What is an appropriate law enforcement use for a drone? When do you have to have a warrant? [At what point] does it invade [our] privacy?
- Dianne Feinstein, Chairman of the Senate Intelligence Committee.[47]

A. *Current Federal Framework*

1. Federal Aviation Administration Regulations

The Federal Aviation Administration, will have a role to play in regulating privacy—albeit a very limited one. The reason for this limited role is due to the limited nature of its regulatory responsibilities. It was created in 1958 to promote the safe and efficient use of the U.S. airways, *not* to protect privacy or advance the cause of civil liberties. Accordingly, the FAA has remained true to this objectives and consistently stated "its mission does not include developing or enforcing policies pertaining to privacy or civil liberties."[48] Consequently,

[44] Stepanovich, *supra* note 41, at 17.
[45] ACLU, *supra* note 25, at 59.
[46] ACLU, *supra* note 25, at 59.
[47] Diane Feinstein, *Drones Over America* (Transcript), 60 Minutes: CBS News, (Jun. 22, 2014), http://www.cbsnews.com/news/drones-over-america-2/.
[48] Thompson, *supra* note 33, at 18. (citing See Federal Aviation Administration, Integration Of Civil Unmanned Aircraft Systems (UAS) In The National Airspace System (NAS) Roadmap 11 (Nov. 7, 2013), https://www.faa.gov/uas/legislative_programs/uas_roadmap/media/UAS_Roadmap_2013.pdf.). Many have called

although the FAA will be responsible for authorizing drones usage through its provision of Certificates of Authorizations it will not expand its regulatory powers to incorporate matters of privacy concern into its decision-making calculus.[49] As the FAA once again reaffirmed in its 2015 release of its latest operating requirements, privacy concerns remain "beyond the scope of [its] rulemaking."[50]

2. 2015 Department of Justice & Presidential Memoranda on Drones

In response to this regulatory void, President Obama issued a memorandum on February 15, 2015 instructing all federal agencies to evaluate the privacy impact of its use of drones and to develop policies to mitigate citizens' privacy concerns as much as possible.[51]

The memorandum instructs agencies to refrain from retaining information that includes personally identifiable information for more than 180 days and instructs agencies to carefully restrict the dissemination of its collected information as well.[52] To ensure accountability, the memo calls for agencies to develop procedures to: 1) "receive, investigate and address" privacy complaints; 2) ensure adequate training for government personnel; 3) establish oversight for

---

for the FAA to provide a greater degree of "inter-agency coordination to close the UAS privacy gap" and clarify "jurisdictional bounds" "responsibilities" and necessary accountability for successful UAS integration. Pratice Hendriksen, *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat Through Interagency Coordination*, 82 GEO. WASH. L. REV. 207, 233 (2013) (calling for Congress to to revise the FAA modernization and Reform Act to require greater intra-agency coordination).

[49] These Certificates of Authorization from the FAA require "detailed information about each flight, including the technology involved, the location of the fight, and training of [each of the] individuals involved." Nate Vogel, *Drones at Home: The Debate Over Unmanned Aircraft in State Legislatures*, 8 ALB. GOVT. L. REV. 204, 228 (2015). http://www.albanygovernmentlawreview.org/Articles/Vol08_1/8.1.204-N.%20Vogel.pdf. Prior to certifying the application, the FAA conducts a comprehensive operation and technical review of the drone to ensure its safety and integrity.

[50] Thompson, *supra* note 33, at 19. (citing Notice of Proposed Rulemaking, Operation and Certification of Small Unmanned Aircraft Systems, Federal Aviation Administration (Feb. 15, 2015), available at http://www.faa.gov/regulations_policies/rulemaking/ recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf.

[51] Thompson, *supra* note 33, at 19 (citing Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, And Civil Liberties In Domestic Use Of Unmanned Aircraft Systems (Feb. 15, 2015). https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua).

[52] *Id.*

access to "sensitive information"; and 4) develop clear guidelines for loaning out drones to other agencies to ensure that adequate safeguards are in place.[53] To promote greater transparency, the memorandum additionally requires agencies to provide public notice of all its authorized uses in a yearly summary.[54]

Lastly, on May 22, 2015 the Department of Justice supplemented the President's Memorandum with an agency-wide memorandum of its own, offering additional policy guidance for the Federal use of drone technology.[55] The DOJ's memo stated that all agencies are strictly prohibited from monitoring protected First Amendment activities and must ensure that personnel operating drones are "appropriately trained and supervised."[56] The DOJ's memo also calls for "annual privacy reviews" to "ensure compliance with the department policy, existing laws and regulations, and to identify potential privacy risks."[57]

Nevertheless, however salutary and prophylactic the Presidential and DOJ memoranda may appear in theory,[58] until they are actually formulated, established, and implemented at each particular agency, the responsibility for regulating drones will largely devolve upon Congress, the Courts, and the various States to generate, formulate, and define. This is particularly true

[53] Thompson, *supra* note 33, at 19.
[54] *Id.* at 20.
[55] DOJ, *Department of Justice Establishes Policy Guidance on Domestic Use of Unmanned Aircraft Systems*, (May 22, 2015), http://www.justice.gov/opa/pr/department-justice-establishes-policy-guidance-domestic-use-unmanned-aircraft-systems.
[56] DOJ, *Department of Justice Establishes Policy Guidance on Domestic Use of Unmanned Aircraft Systems*, (May 22, 2015), http://www.justice.gov/opa/pr/department-justice-establishes-policy-guidance-domestic-use-unmanned-aircraft-systems.
[57] *Id.*
[58] As one commentator on the memo noted, "Because the memo's requirements are not specific, the drone policies the agencies set for themselves" will actually in large part determine "how individual's privacy [will ultimately be] protected" in the absence of Congressional action setting "strong privacy and transparency standards for drone use." Harley Geiger, *White House Drone Memo Right to Focus on Privacy, Center for Democracy and Technology*, Center for Democracy & Technology (Feb. 15, 2015), https://cdt.org/press/white-house-drone-memo-right-to-focus-on-privacy/.

since there appears to be a significant internal discord between the policy positions promulgated by the FBI and ATF on the one hand[59] and the DOJ Inspector General[60] on the other.[61]

3. Proposed Congressional Bills

To date, Congress has not yet enacted any substantive drone legislation pertaining to either privacy or national security. However, in the Spring of 2013 and Winter of 2014, multiple hearings were held in the House and Senate to determine the best course of action for drone regulation moving forward.[62] Shortly thereafter, various forms of drone regulation were proposed in both the House and Senate. The three most notable Federal bills proposed were by Representative Ted Poe, Senator Ed Market, and Senator Rand Paul respectively.

Congressman Poe's House bill called "Preserving American Privacy Act of 2013 (H.R. 637), proposed a warrant requirement for police based on "specific and articulable facts showing a reasonable suspicion of criminal activity."[63] The permitted exceptions to this requirement included circumstances that involved: 1) border patrol situations 2) threats of terrorist attacks or

---

[59] Unlike the DOJ, the FBI and ATF both informed the IG's office that they do not see a practical difference between how a drone collects evidence and how manned aircrafts collect evidence and would not rule out warrantless surveillance because drones do not physically trespass on property. Thompson, *supra* note 33, at 22. (citing U.S. Dep't of Justice, Office of the Inspector General, Interim Report on the Department of Justice's Use and Support of Unmanned Aircraft Systems ii (2013), http://www.justice.gov/oig/reports/2013/a1337.pdf.; *see also* The Associated Press, *Justice Department Spent Nearly $5M on Drones,* CBS News (Sept. 26, 2013) http://www.cbsnews.com/news/justice-department-spent-nearly-5m-on-drones/

[60] According to the DOJ Inspector General's assessment, there were in fact significant differences between manned and unmanned aircraft operations which he concluded would require a different policy analysis. The Inspector General explained:

> We found that the technological capabilities of UAS and the current, uncoordinated approach of DOJ components to UAS use may merit the DOJ developing consistent, UAS-specific policies to guide the proper use of UAS. Unlike manned aircraft, UAS can be used in close proximity to a home and, with longer-lasting power systems, may be capable of flying for several hours or even days at a time, raising unique concerns about privacy and the collection of evidence with UAS. Considering that multiple components are using or have the potential to use UAS, we believe the Office of the Deputy Attorney General (ODAG), which has the primary responsibility within DOJ for formulating cross-component law enforcement policies, should consider the need for a DOJ-wide policy regarding UAS uses that could have significant privacy or other legal implications. *Id*. at 22.

[61] *Id.*

[62] *Id.* at 247.

[63] *Id.* Ted Poe, H.R. 637, Preserving American Privacy Act of 2013, https://www.govtrack.us/congress/bills/113/hr637/text.

3) other emergency circumstances requiring swift action.[64] The ACLU has expressed enthusiastic support for the bill, stating publically that it believed Poe's proposal offered a sensible way to "guard Americans against being subject[ed] [to] mass surveillance by law enforcement, while still allowing police to benefit from the technology."[65]

Senator Edward Markey's bill "Drone Aircraft Privacy and Transparency Act of 2013," proposed that law enforcement's use of drones would be permissible only pursuant to a warrant based upon "probable cause."[66] Markey's bill additionally proposed several unique provisions including a data collection statement,[67] data minimization statement, revocation sanctions for misuse, and various enforcement mechanisms for civil suits against the government.[68] Markey's bill recognized exceptions for "exigent circumstances" involving "imminent danger[s]" or for high risks of "terrorist attack[s]."[69] Otherwise, it states that the governmental may not use a drone to collect data or information of any kind except pursuant to a warrant or unless otherwise permitted under the Foreign Intelligence Surveillance Act of 1978.[70]

Lastly, Senator Rand Paul's bill, "Preserving Freedom from Unwarranted Surveillance Act," like Markey's proposal prohibits all evidence collected by drones from being used in a criminal proceeding unless obtained pursuant to a warrant based upon probable cause.[71] The bill grants exceptions for 1) patrol of the borders for illegal persons or substances, 2) exigent

---

[64] *Id.*

[65] Sandra Fulton, *Experts Discuss Surveillance Society at Domestic Drones Hearing*, ACLU Washington Legislative Office, (May 17, 2013) https://www.aclu.org/blog/experts-discuss-surveillance-society-domestic-drones-hearing.

[66] S. 635, Drone Aircraft Privacy and Transparency Act, 114 Congress (2015-2016).

[67] This data collection statement must include: the individuals or entities that will have the power to use the drone, the specific locations in which it will operate, the maximm period for which it will operate each flight and the nature information or data it will collect and its use. Markey, S. 1639 Drone Aircraft Privacy and Transparency Act of 2013 at § 339 (b) 1-4. https://www.congress.gov/bill/113th-congress/senate-bill/1639/text.

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] Proposed Bill S. 3287, *Preserving Freedom from Unwarranted Surveillance Act of 2012*, https://www.govtrack.us/congress/bills/112/s3287/text.

circumstances, and 3) "to counter a high risk of a terrorist attack."[72] Additionally, like Markey's bill it provides remedies for violations of its provisions by creating a right for an "aggrieved party" to sue in a civil proceeding against the government and the right to prohibit the use of evidence obtained in violation of the bill "in a criminal prosecution.[73] In sum, the proposals share many commonalities as well as many distinctive features and only time will tell which course of regulatory action Congress will ultimately decide to take.

4. Federal Use of Drones to Date

Despite the regulatory void in this area, this has not kept federal agencies from testing the waters with drone technology. On the contrary, drones have been employed in the domestic skies on hundreds of occasions[74] within the past several years by federal, state and local agencies alike.[75] Most of these missions were performed by the Coast Guard, the Drug Enforcement Administration and Immigration authorities for aiding "disaster relief," conducting search and rescue missions,[76] and investigating marijuana production and methamphetamine laboratories.[77] Yet, as FBI Director Robert Mueller frankly admitted in revealing 2013 Congressional hearing by and large these agencies have not yet established any strict policies or any "operational guidelines" to govern their use.[78] Consequently, given the inchoate stage of Federal drone

[72] *Id.*

[73] Proposed Bill S. 3287, *Preserving Freedom from Unwarranted Surveillance Act of 2012*, https://www.govtrack.us/congress/bills/112/s3287/text.

[74] All told, roughly 700 Federal domestic surveillance missions were conducted by drones on loan from the Customs and Border Protection agency between 2010 and 2012. Craig Whitlock & Craig Timberg, *Border-Patrol Drones Being Borrowed By Other Agencies More Often Than Previously Known*, THE WASHINGTON POST (Jan. 14, 2014).

[75] John C. Blakeman, *Drones and Police Practices* in PRIVACY IN THE DIGITAL AGE, 199, 201(eds. NANCY S. LIND & ERIK RANKIN 2015).

[76] *Id.*

[77] Craig Whitlock & Craig Timberg, *Border-Patrol Drones Being Borrowed By Other Agencies More Often Than Previously Known*, THE WASHINGTON POST (Jan. 14, 2014).

[78] Blakeman, *supra* note 75, at 205; Jason Koebler, *FBI Uses Drones for Survillance, Without Clear Guidelines,* US News & World *Report* (June 19, 2013) http://www.usnews.com/news/articles/2013/06/19/fbi-uses-drones-for-surveillance-without-clear-guidelines.

legislation, many believe that Congress will look to the States for guidance in implementing the most effective framework for drone regulation.

B. *State Laws*

In 2013, Virginia became the first state to pass drones regulation, when it enacted a two year moratorium banning all non-emergency governmental drone use.[79] Idaho quickly followed suit and passed legislation that mandated a warrant requirement based upon probable cause with various exceptions for emergency responses, search and rescue missions, and controlled substance investigations.[80]

Since then, many states have introduced proposals and enacted a wide variety of drone regulations. On the one hand, states like Idaho and Kansas currently permit law enforcement surveillance under a lesser standard than probable cause, requiring " a reasonable articulable suspicion of criminal conduct" in Idaho and "specific and articulable facts demonstrating reasonable suspicion of criminal activity" in Kansas.[81] On the other hand, bills like Georgia's H.B. 560 require law enforcement officials to get a warrant based upon probable cause before operating an unmanned aircraft "for any purpose whatsoever within the airspace of the State of Georgia" with "misdemeanor" sanctions for officials who violate its provisions.[82] Additionally, there is a great variety in the number of exceptions permitted to the warrant requirement as well.

[79] They voted for a two-year moratorium on law enforcement agencies use of drones until 2015, with carve out exceptions for major disasters, Amber Alerts, and search and rescue missions. Idaho soon followed suit several months later and became the first state to explicitly enact a law regulating the use of drones by law enforcement officials (as opposed to merely delaying the use two-years in the case of Virginia). Like many of the Federal proposals before it, Idaho's law requires public entitles to obtain a search warrant in order to gather evidence or collect information about an individual in anticipation of a criminal prosecution. The bill provides exceptions for emergence responses, search and rescue missions, and controlled substance investigations. See Allie Bohm, The First State Law on Drones, ACLU (April 15, 2013) https://www.aclu.org/blog/first-state-laws-drones. It should be noted that this latter exception for "controlled-substance investigations" is fairly unique and has not generally been replicated by many of the other states that have considered the issue. *Id.* Weiden, *supra* note 36, at 250-51.

[80] *Id.*

[81] IDAHO CODE ANN. § 21-213 (West 2013);

[82] GEORGIA H.B. 560, http://www.legis.ga.gov/Legislation/20132014/133688.pdf.

Arkansas, Hawaii, Maine, and Michigan take a very deferential approach to warrant exceptions including one bill that excludes circumstances relating to matters as broadly defined as "conspiratorial activities threatening the national security interest … or characteristic of organized crime."[83] More expansive still, Texas drone regulation currently possesses over nineteen expressly recognized exceptions to its warrant requirement and has accordingly been criticized by privacy-advocates as tantamount to regulatory "Swiss cheese."[84] On the other hand, many State bills stringently restrict "the time, place and manner of drone operation" with the most typical restriction providing a forty-eight hour window for the mission.[85]

It should be duly noted that ambitious bills like Georgia's H.B. 560, may run afoul of Federal preemption laws given their purportedly broad regulatory reach.[86] Nevertheless, as this brief survey suggests the State proposals to date vary considerably in the respective privacy coverage they attempt to provide as well as the degree of security exceptions they permit.[87] Consequently, in the uncertainty created by Congressional inaction and the variety of State

[83] Colonel Dawn M.K. Zoldi, *Drones at Home: Domestic Drone Legislation – A Survey, Analysis and Framework*, 4 U. MIAMI NAT'L SECURITY & ARMED CONFLICT L. REV. 48, 59 (2014).

[84] Morgan Smith & Maurice Chammah, *Adding Exemptions: Texas Senate Approves Drone Bill*, (May 17, 2013) http://www.texastribune.org/2013/05/17/senate-panel-passes-drone-bill/; Notably, Dawn Zoldi has commented that many State bills do not mention the U.S. military as exempt and thus could create significant difficulties for "military training, operations and combat readiness." Colonel Dawn M.K. Zoldi, *Drones at Home: Domestic Drone Legislation – A Survey, Analysis and Framework*, 4 U. MIAMI NAT'L SECURITY & ARMED CONFLICT L. REV. 48 (2014).
Moreover, according to Zoldi's analysis about one third are ambigious enough to implicate the Department of Defense as well. *Id.* at 53.

[85] *Id.* at 61.

[86] Nate Vogel, *Drones at Home: The Debate Over Unmanned Aircraft in State Legislatures*, 8 ALB. GOVT. L. REV. 204, 256-257 (2015).(The Supreme Court has articulated three cases which involve Federal preemption: "First, federal law preempts when the federal statute explicitly states that it preempts conflicting state laws. Second, federal law preempts state law when the state law 'regulates conduct in a field that Congress intended the Federal Government to occupy. [Third] when a state law "actually conflicts with federal law . . . [i.e.] where it is impossible for a private party to comply with both state and federal requirements[.]') *Id*.

[87] Colonel Dawn M.K. Zoldi, *Drones at Home: Domestic Drone Legislation – A Survey, Analysis and Framework*, 4 U. MIAMI NAT'L SECURITY & ARMED CONFLICT L. REV. 48, 70 (2014). (concluding, "The collective result of these disjointed state policies is that suspects will likely benefit from [various] procedural windfalls; lives and property may be lost for fear of personal liability; [and] military training and operations will be degraded to the detriment of our greater society.").

regulatory schemes currently in place the courts will inevitably be called upon to clarify the applicability of the Fourth Amendment and establish the floor for Constitutionally permissible drone use.

III.
JURISPRUDENTIAL FRAMEWORK: DRONES & THE FOURTH AMENDMENT

Time works changes, brings into existence new conditions and purposes ... This is peculiarly true of constitutions ... In the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be. Under any other rule a constitution would indeed be ... deficient in efficacy and power ... converted by precedent into impotent and lifeless formulas. Rights declared in words might be lost in reality. – Justice Brandeis[88]

The Fourth Amendment's prohibition against unreasonable searches and seizures has endured for over two centuries through periods of significant social turmoil, political upheaval, and drastic technological change. For more than 40 years between the roaring twenties and the tumultuous 1960s, "a physical trespass" test was applied to determine the scope of its protections.[89] From the late 1960s up to the present day the Court's has applied a two pronged test that first assesses whether an individual's subjective "expectation of privacy" was violated and second determines whether society is ready to recognize that expectation as legitimate. Nevertheless, despite various changes in the test's requirements, "the touchstone" of this inquiry from founding era to the present day has always been a determination of "reasonableness."[90]

Accordingly, by locating this unique historical evolution of "reasonableness" within the technological revolution that is currently underway, I contend that Fourth Amendment is primed to undergo yet another significant paradigm-shift with the introduction of drones into our

[88] Olmstead v. U.S. 438, 473 (1928)(Brandeis, J., dissenting).
[89] Grassley, *supra* note 41, at 4.
[90] Thompson, *supra* note 35, at 2.

domestic skies.[91] In sum, the prevailing property and expectation-bound principles of our current Fourth Amendment jurisprudence will be shaken by the coming earthquake that is drone technology—and the fault lines created by these tectonic shifts will present fresh, new possibilities for privacy protection to emerge and reconfigure the jurisprudential topography in profoundly significant ways.

A. Early History

In order to properly understand why the Fourth Amendment is primed to be revolutionized it is first important to recognize how the test has changed since its original enactment in the 19th century. Although, its central meaning has remained relatively constant—as reasonableness has always been its guiding light—it has also evolved and adapted in many ways to harmonize the needs of changing times with the enduring values that originally animated the Founding Fathers to protest against the British tyranny, take up arms against their mother country, and establish a new form of government *of, by and for* the people.

This historical dimension of the Fourth Amendment is often forgotten in modern times. It was, however, the British tyranny of general warrants that originally set off the powder keg that began the American revolution.[92] These writs of assistance, also known as general warrants, permitted British officers to conduct highly offensive searches without first establishing probable cause. In practice, these searches became tantamount to veritable "fishing expeditions" fraught with officer abuse.[93] Reflecting back on this period, our nation's second President John Adams

[91] Many experts have come to realize that recent developments in Fourth Amendment jurisprudence coupled with the ability of drones to provide unprecedented surveillance "may lead to new standards establishing Fourth Amendment violations." *Id.*

[92] *See* STEPHEN DYCUS et al., NATIONAL SECURITY LAW: FIFTH EDITION, 554 (2011).

[93] STEPHEN DYCUS et al., NATIONAL SECURITY LAW: FIFTH EDITION, 554 (2011). ("The British general warrant was a search tool employed without limitation on location, and without any necessity to precisely describe the object or person sought."). See DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY vii (1979) ("Abuse of general search warrant … by English authorities in the American colonies led to [the] adoption of the Fourth Amendment subjecting searches and seizures to warrant requirements …").

recalled the impassioned speeches of James Otis in 1761 denouncing the hated British writs of assistance as one of the seminal moment in American history:

> American independence was then and there born; the seeds of patriots and heroes were then and there sown … Every man of the crowded audience appeared to me to go away, as I did, ready to take up arms against writs of assistance. Then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born. In fifteen years, namely in 1776, he grew up to manhood, and declared himself free.[94]

Accordingly, with this virtually "unfettered discretion," general warrants "could be, and often were," used to "intimidate" American colonist in demeaning and pernicious ways.[95] Consequently, the Framers sought to protect individual freedom and privacy from precisely that kind of broad and unconstrained discretion when they enacted the Fourth Amendment which states that:

> 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.[96]

Over time, the amendment has been interpreted to require essentially three elements in order to be valid: "probable cause,[97] judicial approval,[98] and particularity[99]."[100] By understanding this unique history, we can better appreciate how the Fourth Amendment was successfully

---

[94] John Adams, *Letter to William Tudor*, THE WORKS OF JOHN ADAMS: VOLUME 10 (LETTERS 1811-1825, INDEXES) (Mar. 29, 1817)[1854]. http://oll.libertyfund.org/titles/2127

[95] William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 Am. U. L. rev 1, 92-94 (2001).

[96] U.S. CONST., AMEND. IV.

[97] United States v. Grubbs 547 U.S. 90, 95 (2006)("Probable cause exists when there is a fair probability that contraband or evidence of a crime will be found in a particular place. Because the probable-cause requirement looks to whether evidence will be found when the search is conducted, all warrants are, in a sense, anticipatory.")

[98] *Id.* at 99 ("The Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant, but by interposing, ex ante, the deliberate, impartial judgment of a judicial officer between the citizen and the police, and by providing, ex post, a right to suppress evidence improperly obtained and a cause of action for damages.")

[99] *Id.* at 97 ("Two matters … must be particularly described in the warrant: "the place to be searched" and "the persons or things to be seized.")

[100] Jennifer O'Brien, *Warrantless Government Drone Surveillance: A Challenge to the Fourth Amendment*, 30 JOHN MARSHALL J. INFO. TECH. & PRIVACY L. 155, 169.

framed in direct response to the fears of abusive general warrants. This is highly instructive and insightful in our current day and age—where the possibility of intrusive searches is far greater than British guards aimlessly rummaging through our papers and far more devastating as well since they can be accomplished surreptitiously without the use of force and without awareness that an invasion has ever even occurred.[101]

B. Olmstead and Incorporation

Because the Bill of Rights did not initially apply to the states prior to the passage of the Fourteenth Amendment and because "federal criminal investigations were less common in the first century of the nation's history" a great deal of the Fourth Amendment's body of law did not develop until well into the 20th century.[102] As one of the first cases to explore the modern contours of this Constitutional right *Olmstead v. United States* was a landmark case and watershed moment in the Courts history that ultimately determined the standard for searches and seizures for the next forty years of American legal history. This decision was largely predicated on a narrow construction of the meaning of a "search" which required a physical trespass in order to trigger Constitutional scrutiny. The Court explained its interpretive approach in this way:

> The amendment itself shows that the search is to be of *material things*-the person, the house, his papers, or his effects … [and] cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."[103]

[101] Banks, *supra* note 95, at 3. (citing James Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 69- 70 (1997).

[102] American History USA, *Fourth Amendment of the U.S. Constitution*, http://www.americanhistoryusa.com/topic/fourth-amendment-to-the-united-states-constitution/

[103] Olmstead v. United States, 277 U.S. 438, 465 (1928)(holding that the Fourth Amendment's protections against unreasonable searches and seizes did not apply to the use of evidence of wiretaps).

Over a decade later in *Goldman v. United States*,[104] the Supreme Court once again reinforced this physical-trespass paradigm in holding that no search occurred when officers utilized a detectaphone to eavesdrop in on a conversation taking place in the building next door.[105] The Court stated that since there was no physical entry upon the defendant's office the government did not violate the defendant's rights under the meaning of the Fourth Amendment.[106] Moreover, the court provided additional gloss on the *Olmstead* physical trespass framework by emphatically rejecting the defendant's petition to distinguish *Olmstead* explaining, "no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the *Olmstead* case ... nothing now can be profitably added … [and] we adhere to the opinion there expressed."[107]

Fast-forward to 1961 and the Supreme Court at last incorporated this limited, through still meaningful Constitutional right against the respective states.[108] Ultimately, however, as modern technology continued to advance *Olmstead* appeared increasingly outdated and was primed to be supplanted in the second half of the 20th century.

C. The Modern Fourth Amendment Test: Reasonable Expectations of Privacy

In the landmark 1967 case of *Katz v. United States*, the Supreme Court significantly departed from its traditional precedents and repudiated *Olmstead's* "narrow view"[109] of the Fourth Amendment by emphatically declaring that, "The Fourth Amendment protects *people*—

---

[104] Goldman v. United States 316 U.S. 129 (1942) (holding that "the use of the detectaphone by Government agents was not a violation of the Fourth Amendment.").

[105] *Id.*

[106] *Id.*

[107] *Id.* at 136.

[108] Mapp v. Ohio, 367 U.S. 643, 660 (1961).

[109] Katz v. United States, 389 U.S. 347, 352-53 (1967)("It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry … but the premise that property interests control the right of the Government to search and seize has been discredited. Thus, although a closely divided Court supposed in Olmstead that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested").

not simply [places]—against unreasonable searches and seizures."[110] The Court continued, "[It may be true] what a person knowingly exposes to the public, even in his own home or office, 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."[111] Finally, directly confronting the holding of *Olmstead* the Court resoundingly proclaimed that, "the reach of that Amendment cannot [reasonably be construed to] turn upon the presence or absence of a physical intrusion into any given enclosure."[112]

Interestingly, however, it was Justice Harlan's formulation of the Fourth Amendment's privacy protection that ultimately carried the day.[113] In his concurring opinion, Justice Harlan promulgated the two-pronged test that the Court later formally adopted in *Smith v. Maryland*:

> Application of the Fourth Amendment depends on whether the person invoking its protection can claim a "legitimate expectation of privacy" that has been invaded by government action. This inquiry normally embraces two questions: first, whether the individual has exhibited an actual (subjective) expectation of privacy; and second, whether his expectation is one that society is prepared to recognize as "reasonable."[114]

Nevertheless, despite the fact that the *Katz* court categorically stated that the Fourth Amendment protects "people not places"—the location of the search has in fact borne heavily on the court's analysis.[115] In other words, the principle "did not create the expected privacy bubble" that civil-liberties groups had hoped for but instead was narrowly interpreted with Harlan's

---

[110] *Id.*

[111] *Id.*

[112] *Id.* at 353. ("We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling … The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.")

[113] Katz, 389 U.S 347, 361-62 (Harlan, J., concurring). ("This case requires us to reconsider Goldman, and I agree that it should now be *overruled.* Its limitation on Fourth Amendment protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion … 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.")

[114] *Smith v. Maryland*, 442 U.S. 735, 735 (1979)(citing *Katz,* 389 U.S. 347, 361)(Harlan, J., concurring).

[115] *Id.*

important qualification in mind that, "what protection [the Fourth Amendment] affords to those people . . . requires reference to a 'place.'"[116] Consequently, as one commentator noted:

> As *Katz* was used as a precedent in [the] case[s] … that followed, time and time again the courts recognized a reasonable expectation of privacy when the intrusions concerned the home—but not when the person or their communications were in public spaces, in effect reintroducing the property-based definition of privacy [that it supposedly repudiated] *through [the] back door*![117]

With these developments in mind we now turn to the recent cases that will bear most heavily on the Court's determination of the constitutionality of domestic drone surveillance—the manned aerial surveillance cases.

D. Manned Aerial Surveillance Cases

The trilogy of manned aerial surveillance cases decided in the late 1980s established a highly deferential standard for police use of aerial surveillance technology. In all three cases the Court upheld the government's use of warrantless aerial surveillance technology and established the general principle that so long as "the government is conducting the surveillance from public navigable airspace, in a non-physically intrusive manner" it is presumptively Constitutional.[118]

In the first aerial surveillance case *California v. Ciarola,*[119] the Court sought to determine whether police could permissibly fly at an altitude of 1000 feet to investigate the production of marijuana over private property. The court held that the search by police did not violate the Fourth Amendment since the evidence obtained was clearly "visible to the naked eye" and "knowingly expose[d] to the public."[120] The court explained that the Fourth Amendment's

---

[116] Katz, 389 U.S 347, 361 (Harlan, J., concurring).

[117] Amitai Etznioni, *Essay: Eight Nails into Katz's Coffin*, 65 CASE WESTERN RESERVE L. REV. 413, 416 (2014).

[118] Gregory McNeal, *Drones and Aerial Survillance: Considerations for Legislators*, CENTER FOR TECHNOLOGY INNOVATION BROOKINGS INSTITUTE, (Nov. 2014), http://www.brookings.edu/~/media/Research/Files/Reports/2014/10/drones-aerial-surveillance-legislators/Drones_Aerial_Surveillance_McNeal_FINAL.pdf?la=en.

[119] 476 U.S. 207 (1986).

[120] *Id.*

steadfast protection of the home has never been extended to "require law enforcement officers to shield their eyes" from what is clearly visible in plain sight to the general public.[121]

Consequently, two principles can be extrapolated from this case. First, whatever is clearly visible within the plain view of the public is not protected under the Fourth Amendment—*even if*—it is only visible from an aerial viewpoint. Secondly, it highlights what has become known as the "knowing-exposure doctrine" which means that whatever an individual "knowingly exposes" to the public even in "his [or her] own home or office" will not trigger Constitutional scrutiny.

The second case in the aerial surveillance trilogy, *Dow Chem. Co v. United States,*[122] involved a industrial manufacturing plant that refused to allow the Environmental Protection Agency to investigate its property. The EPA subsequently decided to hire an aerial photographer to survey the property. The court ultimately held that, "The taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[123] It noted, however, that police surveillance of private property "using highly sophisticated surveillance [technology] not generally available to the public" would likely require closer scrutiny but in the present case "the photographs [were] not so revealing of intimate details as to raise [serious] constitutional concerns."[124] Additionally, the court significantly observed that, "An electronic device [capable of] penetrat[ing] walls or windows so as to hear and record confidential discussions … would raise very different and far more serious questions."[125] Accordingly*, Dow Chemical* adds several additional factors for analyzing the Constitutionality of drone surveillance technology: (1) the degree of sophistication of the

[121] *Id.*
[122] 476 U.S. 227, 239 (1986).
[123] *Id.*
[124] *Id.*
[125] *Id.* at 238-39.

technology, (2) the extent to which it is invasive and (3) the extent to which that technology is generally available to the public at the time of its operation.

The third and final aerial surveillance case, *Florida v. Reilly,* was a plurality decision and merely reinforced the prevailing doctrines established in *Ciaralo* and *Dow Chemical*. The plurality held as it had previously in *Ciaralo* that the police observation of contraband "clearly visible to the naked eye" from an altitude of 400 feet does not violate the Fourth Amendment.[126] Accordingly, *Reilly* provides additional gloss on *Ciaralo* and *Dow*—what is visible to the naked eye is presumptively permissible for police to observe.

One commentator succinctly summarized the doctrinal upshot of these three aerial surveillance cases in this way, "As long as the police are [conducting surveillance from] a lawful vantage point, they can use [non-invasive] technology to spy on anything occurring in public spaces or on private property outside the home without [violating] the Fourth Amendment."[127]

E. New Technology in Recent Fourth Amendment Surveillance Cases

More recent 21st century Supreme Court cases, however, make forecasting the Court's prospective framework for drones considerably more difficult. In three different cases involving novel methods of investigation the court struck down the use of thermal-radar technology to identify marijuana in an individual's home, GPS technology to track a defendant's movements over the course of two months, and drug-sniffing dogs to search the curtilage of one's home.

---

[126] *Id.*

[127] Christopher Slobogin, *Is the Fourth Amendment Relevant*, in CONSTITUTION 3.0, 14 (eds. Jeffrey Rosen & Benjamin Wittes 2011). See also Joseph J. Vacek, *Big Brother Will Soon Be Watching—Or Will He: Constitutional Regulatory, and Operational Issues Surround the Use of Unmanned Aerial Vehicles in Law Enforcement*, 85 N.D. L. REV. 673 (2009) (stating a bit more provocatively, "Constitutionally, it seems that aerial surveillance by any method of any area in open view from any legal altitude does not implicate the Fourth Amendment, so long as the technology used to obtain the surveillance … is in general public use and does not penetrate into the home."). See also Matthew R. Koerner, *Drones and the Fourth Amendment*, 64 Duke L. J. 1129, 1146 (2015) (concluding that "drones will maneuver through each and every loophole" of Fourth Amendment jurisprudence.)[127]

In the first case of *Kyllo* v. United States,[128] the Supreme Court had its first opportunity to expound upon the "highly sophisticated surveillance technology" that it warned might violate the Fourth Amendment in *Dow Chemical*. In this case, police decided to utilize new thermal imaging technology to examine whether the defendant was growing marijuana on his property. The Court held that, "Where the government uses a device that is not [with]in [the] general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[129] Nevertheless, some have called the Court's ruling in *Kyllo* a "pyrrhic victory for privacy," since what was gained through recognition of the violation may very well have been lost with reinforcement of various theories like the "plain-view" and "knowing-exposure" doctrines which civil liberties proponents believe do a grave disservice to privacy.[130]

In *Jones v. United States*,[131] the Court encountered another novel use of technology—the attachment of a GPS tracking device to monitor the defendant's movement's over a two-month period of time. The *Jones* Court held that, "the Government's installation of a GPS device on a target's vehicle and its use of that device to monitor the vehicle's movements, constituted a "search" under the meaning of the Fourth Amendment.[132]

It should be noted that the Court resurrected the *Olmstead* test of physical trespass to decide the case on originalist grounds. The court conceded that although new theories of privacy may emerge in the future—the physical trespass test continues to be a viable means for establishing "at a minimum" that a search has taken place of a "constitutionally protected area"

[128] Kyllo v. United States, 533 U.S. 27, 29 (2001).
[129] *Id.*
[130] Christopher Slobogin, *Is the Fourth Amendment Relevant*, in CONSTITUTION 3.0, 16 (eds. Jeffrey Rosen & Benjamin Wittes 2011).
[131] 132 S.Ct. 945, 949 (2012).
[132] United States v. Jones, 132 S.Ct. 945, 949 (2012).

under the original meaning of the Fourth Amendment as ratified by the Founders.[133] In other words, the court clarified that the *Olmstead* test for physical trespass was *augmented* by Katz two-pronged test and *not* replaced by it.[134]

Justice Sotomayor's concurring opinion is particularly noteworthy insofar as it adumbrates the future course the court may take when drone at last arrive on their docket. Justice Sotomayor notably observed that, "cases involving even short-term monitoring ... require particular attention" because the "Government can store such records and efficiently mine them for information years into the future."[135] Moreover, Justice Sotomayor observations appear particularly salient for forecasting the court's response to drones since like GPS tracking, drones too are relatively "cheap," "proceed surreptitiously," and "evade the ordinary checks" that have traditionally constrained "abusive law enforcement practices," namely "limited police resources and community hostility.'"[136]

Justice Alito's concurring opinion also made very significant remarks that will likely prove seminal in the first drone case to arrive on the Supreme Court docket. In his concurring opinion joined by Justice Breyer, Ginsberg and Kagan he expressed his concerns regarding *Katz's* subjectivity, circularity, and highly dubious sociological assumptions—namely that individuals possess well-developed and stable expectations in spite of copious evidence to the contrary[137]—as all reflecting deeply problematic aspects of the *Katz* test that need to be seriously reexamined in light of modern realities.

---

[133] *Id.* at 950 n.3.

[134] See *Id.* at 946("Whatever new methods of investigation may be devised, the United States Supreme Court's task, at a minimum, is to decide whether the action in question would have constituted a "search" within the original meaning of the Fourth Amendment. Where the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.").

[135] *Id.*

[136] *Id.*

[137] For example, "A 2003 poll, … found that a strong majority (68%) of Americans favored invading Iraq, but this number fell to a minority (43%) if the possibility of U.S. military casualties was mentioned in the question."

Thus, Alito's concurrence considered in conjunction with Justice Sotomayor concurrence, contains at least five votes five votes that would be willing to reconsider the traditional rule that surveillance in public does not constitute a search and on a deeper level re-assess the continuing viability of the *Katz* test altogether.[138] In sum, Justice Sotomayor's arguments dovetailed perfectly with the major themes of Justice Alito's insofar as they both recognize that the Court's continued adherence to *Katz* is "ill-suited" to the considerable challenges posed by "the digital age."[139]

Lastly, in Florida v. *Jardines*, the court again returned to the physical-trespass theory of privacy to to strike down the use of a sense-enhancing, drug-sniffing police dog to investigate the curtilage of a private residence in search of drugs.[140] The Court distinguished the search from the trilogy of aerial surveillance cases by explaining that "in permitting … visual observation of the home we were careful to note that it was done *'in a physically non-intrusive manner*.'"[141]

In sum, the recent technology cases have muddied the jurisprudential waters and made the prospect of making a clear and decisive prediction about how the court will respond to drone technology a much more difficult and complicated endeavor.

Amitai Etznioni, *Essay: Eight Nails into Katz's Coffin*, 65 CASE WESTERN RESERVE L. REV. 413, 416 (2014). Similarly, "a medical study found that patients were almost twice as likely to reject surgery when the predicted outcome was phrased in terms of "mortality rate" rather than 'survival rate." *Id*. These variances based solely on rhetoric alone present formidable obstacles to the Court's determination of what the American people actually expect—when Americans themselves may not even know the answer.

[138] Justice Alito concurrence would have found, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." S. Ct. 945, at 964. (Alito, J., concurring). Likewise Justice Sotomayor stated that extended periods of tracking may "reflect a wealth of detail" about the most intimate details of an individuals life and thus could constitute a violation of privacy under the meaning of the Fourth Amendment. *Id.* at 955. (Sotomayor, J., concurring). Recently the Roberts court reflected a growing awareness of the new challenges of the digital age in Riley v. California in which the Court's unanimous opinion quoted Justice Sotomayor's *Jones* concurrence in the context of suppressing evidence obtained from a warrantless cell phone search and explained how the digital age has changed the nature of privacy ("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…"). Riley, 134, S. Ct. 2473, 2491 (2014).

[139] *Id.*

[140] 133 S. Ct. 1409, 1417-18 (2013).

[141] *Id*.

F. A New National Security Exception?

The last piece of the jurisprudential puzzle is to assess whether any of the existing categories of judicially-recognized exceptions to the Fourth Amendment will apply to domestic drone surveillance or alternatively whether drones may catalyze the creation of an entirely new exception altogether. Accordingly, the three most plausible possibilities would entail either: (1) an expansion of the special needs doctrine, (2) a return to the "pure intelligence rule"[142] to expand the foreign intelligence exception to domestic operations, or (3) the creation of a new "National Security" exception that would consolidate all special needs and intelligence surveillance activities under a single judicially-recognized exception to the Fourth Amendment.

1. Expansion of the Special Needs Exception

If drones will in fact expand the special needs exception they will follow a well-tread path that has been developing for well over three-decades. Historically, the general rule until the late 1960s was that in order for a search to be deemed "reasonable" under the Fourth Amendment, law enforcement officials would first be required to obtain a warrant from a neutral and detached magistrate on the basis of probable cause.[143] Nevertheless, over time the Supreme Court has significantly "loosened this warrant requirement" in circumstances in which a "strict showing of individualized suspicion of probable cause" would be deemed to unduly "hinder"

[142] This was actually the traditional *modus operadi* of the Executive branch. As one commentator has explained: "Well into the 1970s, the executive branch assumed that the national security exception [to the Fourth Amendment] permitted only, in the words of FBI Director J. Edgar Hoover, 'purely intelligence' focused investigations." This "pure intelligence" rule meant that evidence gleaned from warrantless searches and surveillance were "constitutionally inadmissible in subsequent prosecutions." L. Rush. Atkinson, The Fourth Amendment's National Security Exception: Its History and Limits, VAND. L. R. 1343, 1346 (Oct. 2013).

[143] *See* Riley v. California, 134 S.Ct. 2473, 2482 (2014). ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant. Such a warrant ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.").

significant governmental interests.[144] A precursor to the special needs exception was first found in the famous *Terry* case which involved investigation techniques known as the "stop-and-frisk."[145] The court's recognition of the need to conduct searches under "special circumstances" ultimately began the court's shift towards a more flexible, accommodating approach to balancing interests in a variety of settings.[146] In other words, it emerged out of the recognition that "the exclusionary rule has its limitations"[147] and protecting persons from unreasonable searches and seizures aimed at gathering evidence, had distinctive objectives separate and severable from those concerning the prevention of crime and the protection of police officers safety.[148]

Accordingly, the special needs exceptions grew out of this recognition that in the context of safety and administrative regulations: "a search unsupported by probable cause may be [deemed] reasonable when *special needs*, *beyond the normal need for law enforcement*, make the warrant and probable-cause requirement *impracticable*."[149] Since this special needs rationale was first articulated by the court, it has found in favor of upholding the government's interest on almost every occasion it has considered the matter including: "a principal's search of a student in public school,[150] a public employer's search of an employee's office,[151] a probation officer's

[144] Thompson, *supra* note 10, at 11.

[145] Terry v. Ohio, 392 U.S. 1 (1968) (holding that police may constitutionally stop-and-frisk a person if there is a reasonable suspicion that the person has committed or is about to a crime).

[146] *Id*.

[147] *Id*. at 13.

[148] See *id*. at 24, ("In view of these facts, we cannot blind ourselves to the need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest. When an officer is justified in believing that the individual whose suspicious behavior he is investigating at close range is armed and presently dangerous to the officer or to others, *it would appear to be clearly unreasonable to deny the officer the power to take necessary measures to determine whether the person is, in fact, carrying a weapon and to neutralize the threat of physical harm."*)(emphasis added).

[149] Bd. of Educ. v. Earls, 122 S.Ct. 2559, 2564 (2002)

[150] New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

[151] *See* O'Connor v. Ortega, 480 U.S. 709 (1987)

search of a probationer's home,[152] as well as drug testing of railroad employees,[153] Customs Service employees,[154] and high school athletes.[155],,[156]

One has commentator summarized the historical trajectory of the special needs exception in this way, "Since the Pandora's box of special needs was first opened in 1985, the Court's jurisprudence in this area has struggled to find equilibrium. In [sum], the Court [has] applied the exception by invariably finding governmental interests to outweigh privacy concerns."[157] Indeed, if this trend continues and is expanded to encompass domestic drone surveillance the "special needs" exception could soon produce authorized warrantless surveillance so expansive, so pervasive, and so far-reaching as to virtually render the assurances of Fourth Amendment non-existent.

2. Expansion of the Foreign Intelligence Exception

Alternatively, another possibility could arise if the Court's decided to expand the "foreign intelligence" exception to encompass domestic drone surveillance activities as well. The formal recognition of the "foreign intelligence" exception came about fairly recently in a 2008 Foreign Intelligence Surveillance Court (FISC) decision known as *in re Directives.*[158] In that case the court recognized for the first time in American history that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists "when surveillance is conducted to obtain

[152] Griffin v. Wisconsin, 483 U.S. 868 (1987)
[153] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989).
[154] National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).
[155] Vernonia Sch. Dist. 47J v. Acton, 115 S. Ct. 2386 (1995).
[156] Jennifer Y. Buffaloe, *"Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule*, 32 HARV. C.R.-C.L. L. REV. 529, 530 (1997)
[157] Steven R. Probst, Ferguson v. City of Charleston: Slowly Returning the "Special Needs" Doctrine to its Roots, 36 Valparaiso L. Rev. 285, 286 (2001).
[158] In re Directives, 551 F.3d 1004, 1011 (FISA Ct. Rev. Aug. 22, 2008)

foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."[159]

Notably the court arrived at its justification by analogizing from the special needs exception in a way that future courts may apply to accommodate a similar exception for domestic drones. That is to say, despite the fact that the court later cautioned against liberally construing its decision as endorsing "broad-based, indiscriminate executive power" the court's decision may have precisely that sort of effect by both emboldening the Executive Branch to credibly justify extensive use of drone surveillance technology as part and parcel of its "intelligence" gathering responsibilities.[160] In fact, the court gave ample credence to this viewpoint by recognizing "that where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."[161]

Accordingly, the court could extend this logic to permit intelligence officials to conduct domestic surveillance operations on the basis of a revival of the "pure intelligence" rule. In other words, if the intelligence community decided to utilize drones solely for intelligence collection purposes and were prohibited *ex ante* from sharing any evidence acquired by these operations with criminal prosecutors (except for terrorist, espionage or other related matters) then it could

---

[159] *Id.*

[160] In re Directives, 551 F.3d 1004, 1011 (FISA Ct. Rev. Aug. 22, 2008)

[161] *Id.* Many scholars have voiced their concern about the development See Sarah Fowler, *Circumventing the Constitution for National Security: An Analysis of the Evolution of the Foreign Intelligence Exception to the Fourth Amendment's Warrant Requirement*, 4 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 207, 238-40 (2014) ("The foreign intelligence exception began as a narrow tool to shield sensitive national security investigations, but its application has reached an alarming breadth … The Supreme Court has long recognized the necessity of exceptions to the Fourth Amendment's ordinarily strict warrant and probable cause requirements. However, this history illustrates the foreign intelligence exception's glaring disregard for the protections afforded to all Americans by the Fourth Amendment … All three branches of government have fallen short of their constitutional obligations and have let national security completely consume the rest of the Constitution … However compelling the justification of security may be, limitations must be placed on the foreign intelligence exception if the Fourth Amendment is to continue to have any meaning."). *Id*.

conceivable argue for an expansion of the newly created "Foreign Intelligence" exception to encompass domestic matters within its domain as well.

C. Synthesis: Creation of a New National Security Exception?

In summary, there appears to be at least three avenues for domestic drone surveillance to be exempted from the strictures of the Fourth Amendment's warrant requirement. First, if circumstances arose similar to those which gave rise to the special needs exception[162] (i.e. national border related matters,[163] airport screenings, "compliance checks" for private businesses,[164] police roadblocks for drunk-driving,[165] etc.) the court could conceivably argue by analogy to expand the special needs category to accommodate the novel realities of the government's "need" to conduct drone surveillance operations to protect the public safety. Since the court has generally been highly deferential to the Executive branch[166] in circumstances involving the public safety this could result in significant changes in Fourth Amendment law. That is to say, given the courts general hesitancy to interfere in matters pertaining to "serious

[162] It should be noted that prior to the Court's formal adoption the "special needs" exception the court had already by 1985 recognized over twenty exceptions to the probable cause or the warrant requirement or both. *See* Craig Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV 1468, 1474 (1985) ("searches incident to arrest (exceptions to both); automobile searches (exception to warrant requirement); border searches (both); searches near the border (warrant and sometimes both); administrative searches (probable cause exception); administrative searches of regulated businesses (warrant); stop and frisk (both); plain view, open field seizures and prison 'shakedowns' (both, because they are not covered by the fourth amendment at all); exigent circumstances (warrant); search of a person in custody (both); search incident to non-arrest when there is probable cause to arrest (both); fire investigations (warrant);warrantless entry following arrest elsewhere (warrant); boat boarding for document checks (both); consent searches (both); welfare searches (both, because not a 'search'); inventory searches (both); driver's license and vehicle registration checks (both); airport searches (both); searches at courthouse doors (both); the new 'school search' (both); and finally the standing doctrine which, while not strictly an exception to fourth amendment requirements, has that effect by causing the courts to ignore fourth amendment violations."). *Id*.

[163] United States v. Martniez-Fuerte, 428 U.S. 543 (1976).

[164] United States v. Biswell, 406 U.S. 311 (upholding the seizure of defendant's illegal weapons found during a compliance check without a warrant

[165] Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (upholding warrantless searches a police checkpoints).

[166] *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (upholding warrantless searches a police checkpoints)("[F]or purposes of Fourth Amendment analysis, the choice among such reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources, including a finite number of police officers.").

public danger[s]"[167] the Courts may defer to the Executive branches judgment in the sphere of domestic drone surveillance policy for national security related matters. As the Court has stated on several occasions, "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation … while the Constitution protects against invasions of individual rights, *it is not a suicide pact*."[168]

Alternatively, an exception for drones could entail an expansion of the "foreign intelligence" exception for "pure intelligence" activities conducted to investigate persons located *within* the United States, not merely for those reasonable believed to be abroad. This expansion would ingeniously permit the use of warrantless drone surveillance but categorically prohibit its use from being used in criminal prosecutions "to ensure that warrantless intelligence searches remained within the bounds of reasonableness prescribed by the Constitution."[169]

Third and finally, the Court could adopt an altogether new National Security exception, combining both the special needs and foreign intelligence exceptions together under one new consolidated category of judicially recognized exceptions. In other words, courts would "presume a search reasonable if the interest in national security [were] sufficiently strong to justify the intrusiveness of a search."[170] Under such circumstances, a National Security exception could plausibly begin as a narrowly construed carve out—at least at first—and then slowly but steadily expand to encompass more and more permitted searches under its umbrella.[171] When

---

[167] Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 445.

[168] Haig v. Agee, 453 U.S. 280, 307 (1981) (quoting Aptheker v. Secretary of State, 378 U.S. 500, 509 (1964)).

[169] Sarah Fowler, *Circumventing the Constitution for National Security: An Analysis of the Evolution of the Foreign Intelligence Exception to the Fourth Amendment's Warrant Requirement*, 4 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 207, 226 (2014)

[170] Robert F. Greenlee, *The Fourth Amendment and Facilities Inspections Under the Chemical Weapons Convention*, 65 U. CHI. L. REV. 943, 956 (1998).

[171] As several scholars have noted this trend towards expansion of exceptions does not appear to indicate any signs of narrowing in the near future. On the contrary, "Because the security of the nation is such a compelling interest, the foreign intelligence exception appears to be here to stay. Forcing the government to pause a sensitive

this happens—drones collision with the Fourth Amendment may finally reach its point of impact as the requisite powder keg will be at last ignited with the explosive and dramatic results needed to shake up the court, tip the balance of opinion in favor of jettisoning the *Katz* test, and usher in the next epoch of Fourth Amendment privacy law.

G. Drone Jurisprudence

Lastly before synthesizing the material and providing recommendations for drone regulation and jurisprudence, two cases involving domestic drone surveillance have been litigated to date and briefly bear mentioning. The first case avoided the Constitutional issue and the second case did not implicate its strictures since it was solely between private parties.

In the first case, North Dakota SWAT team officials were called in to arrest Rodney Brossart on his North Dakota property after he and three of his family members resisted police officers authorized search warrant to collect six cows that had wandered onto his property.[172] Ultimately, after a sixteen hour marathon standoff ensured, law enforcement officials decided to introduce a Predator drone on loan from the Department of Homeland Security to track the suspects movements on the property.[173] The drone observed the Brossart's 3000 acre farm for just over four hours at an altitude of two miles and transmitted live video feed and thermal images to the officers standing by.[174] When the suspects were discovered to be unarmed the

intelligence investigation to attain judicial approval would certainly frustrate national security aims in many instances." Accordingly, she concludes "It does not seem feasible to reverse the course of history and stymie the evolution of the foreign intelligence exception." Sarah Fowler, Circumventing the Constitution for National Security: An Analysis of the Evolution of the Foreign Intelligence Exception to the Fourth Amendment's Warrant Requirement, 4 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 207, 238-40 (2014)

[172] Jennifer O'Brien, *Warrantless Government Drone Surveillance: A Challenge to the Fourth Amendment*, 30 JOHN MARSHALL J. INFO. TECH. & PRIVACY L. 155, 157 (citing Clay Dillow, For the First Time, Predator Drones Participate in Civilian Arrests on U.S. Soil, Popular Science (dec. 12, 2011) https://ww.popsci.com/technology/article/2011-12/first-us-citizens-have-been-arrested-help-predator-drone.).

[173] *Id.*

[174] *Id.*

officers swiftly moved in and arrested the suspects fortuitously obviating the need to apply force in what may otherwise have been a violent confrontation.[175] When the case finally came before the U.S. District Court in 2012, Judge Joel Medd upheld the warrantless use of drone technology to conduct surveillance, by explaining that "there was no improper use of an unmanned aerial vehicle" and that the drones use " had no bearing on [the] charges being contested."[176] A jury later upheld that decision.[177]

A second case involving private individuals use of drone is also the first of its kind to decide whether an individual's privacy rights are implicated by drones. The Kentucky case involved an alleged Peeping-Tom whose drone had been shot down after the home-owner witnessed the drone repeatedly "spying on his daughter sunbathing."[178] The judge dismissed the criminal charges against the home-owner explaining that, ""it was an invasion of their privacy" and that they "had the right to shoot [down the] drone."[179] The judge explained, "three times in one day, three times over the course of a year, six times total, over one property? That's not right, that's harassment."[180]

Although these cases are very limited in their scope, one can see how difficult it will be for future courts to determine how to decide the flood of cases soon to fill its dockets in the absence of any positive law passed by Congress and the dearth of Supreme Court cases on point. Thus, it is critically important that regulations crafted by legislatures are carefully designed to

---

[175] Blakeman, *supra* note 75, at 202.

[176] *Id.*

[177] Jason Koebler, *North Dakota Man Sentenced to Jail In Controversial Drone-Arrest Case*, http://www.usnews.com/news/articles/2014/01/15/north-dakota-man-sentenced-to-jail-in-controversial-drone-arrest-case (sentencing him to three years and finding Brossart guilty on the charge of terrorizing police).

[178] Anna Giaritelli, *Judge Sides With Man Who Shot Down Drone* http://www.washingtonexaminer.com/judge-sides-with-man-who-shot-down-drone/article/2575323

[179] http://www.theverge.com/2015/10/28/9625468/drone-slayer-kentucky-cleared-charges

[180] Anna Giaritelli, *Judge Sides With Man Who Shot Down Drone* http://www.washingtonexaminer.com/judge-sides-with-man-who-shot-down-drone/article/2575323

advance the nation's security interests while also protecting the right to privacy we hold most dear.[181]

IV.
REGULATING PRIVACY IN THE 21ST CENTURY

Security and privacy are not zero-sum. We have an obligation to give full meaning to both, to protect security while at the same time protecting privacy and other constitutional rights.[182]
- Robert S. Litt, ODNI General Counsel

Federal regulation of drone surveillance is still in its infancy stage, yet the path chartered by Congress will likely have far-reaching effects on society—from National security, to law enforcement effectiveness, to social expectations of privacy and beyond. For this reason, it is essential for policymakers to take an inventory of the critical interests implicated by our schematic approach to regulation and to rationally calculate and weigh the respective costs and benefits. In short, if optimally regulated and employed to their most beneficial use, drones could hold the potential to significantly advance our aspirational efforts to achieve a more safe and secure, prosperous and innovative, dynamic and flourishing shared life together as Americans.

Yet, the safe and secure, free and transparent, entrepreneurial and prosperous society we aspire to be will not come about by mere accident. On the contrary, it must be self-constructed and self-organized—piece by piece, brick by brick, line by line, and take root in the hearts and minds of every citizen. Like the consummate gardener, the law must shape the space it is

[181] As Chief Justice Earl Warren declared,"[O]ur country has taken singular pride in the democratic ideals enshrined in its Constitution... It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties … which makes the defense of the Nation worthwhile." United States v. Robel, 389 U.S. 258, 264 (1967).

[182] Robert S. Litt, *Privacy, Technology and National Intelligence Collection*, An Address by General Counsel of the the Office of the Director of National Intelligence, (July 19, 2013) http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection

responsible for looking after with constant attention, effort, care, and pruning for any garden (or society) to eventually grow, develop, and come into full bloom. In the same way, the kind of society we want to become can and must be shaped by us—the people.

To be sure, the risks of abuse and misuse are very real and must be dealt with directly and decisively with clear, firm, and specific limitations replete with serious sanctions and significant remedial consequences for its violation. These steps will prove absolutely essential for drones to realize their full potential and garner the acceptance and respect of citizens as legitimate instruments of the law capable of furthering socially desirable ends. Nevertheless, the possibility of drones being misused or abused should not blind us to the larger reality of their extraordinary potential for good. In fact, it appears that these development come at the perfect moment in time as State and local budgets grow tighter, our police forces grow thinner, our Federal deficit spirals out of control, and as the aggregate needs of society grow greater and more expansive by the day.

At this crossroads in our nation's history, the manner in which we conceptualize the proper place and role of drones in our society will have profound and enduring significance in shaping our future. I believe it is therefore crucial that we recognize that drones, though powerful and increasingly intelligent, are nothing more than *instruments*—neither good nor evil in and of themselves. How we choose to utilize their power and limit their potential for abuse is entirely up to us. We can self-construct the kind of society we want to live in by selectively shaping the precise contours of the uses of drones that we collectively deem permissible. In short, they can be as productive and beneficial or as harmful and destructive as we—the agents who wield and control their awesome power—permit or direct them to be.

A. Crafting "Smart" Regulations, Not Merely "Strict" Regulations

What is therefore needed most at this watershed moment in our nation's history is "smart" regulations, not simply "strict" ones. The difference is more than mere rhetoric. It connotes a nuanced approach that recognizes how seemingly sensible "strict" regulations on drones can actually function to produce counterproductive outcomes that stymie economic growth, technological development, and innovative uses for drone technology—while simultaneously hobbling police forces, blinding intelligence officials, and shielding criminals and terrorists from exposure to the light of day and the swift and steady hand of justice. What I call "smart" regulation seeks to realize the full potential of socially desirable uses for drone technology while concomitantly limiting their potential for harms through the invasion of privacy, the disclosure of embarrassing or harmful information, or through the unjustified targeting and harassment of unpopular individuals or groups.

Drawing from a variety of literature on the subject as well as various State and Federal proposals, the "smart" regulations I propose in Part A follow an approach I call the "Systematic Schematic of Differentiation" and "The Accountability Apparatus" which entails: (1) tailoring warrant requirement to the location searched, the aims of the particular entity involved, and type of drone utilized along with various (2) minimization protocols; (3) democratic tools for achieving oversight and control; and (4) disciplinary sanctions and civil remedies for violations. Lastly, in Part B, I argue that by tapping into the power of federalism the Federal government can fine-tune its policies to implement and emulate the best-practices from the respective States. In sum, I believe these protocols will go along way in advancing both socially desirable governmental activity and respect for individual privacy without diminishing or compromising either interest in the process. Each element of this "smart" scheme of regulation will accordingly

be examined in turn, before turning to briefly examine the merits of a *Brandeisian* conception of drone regulatory federalism.

1. Systematic Schematic of Differentiation: Tailoring Warrant Requirements to Location, Drone Type & Entity

In this section, I argue that all drone regulation should be narrowly tailored towards the ends for which they are crafted based on the location of the drone search, the entity conducting the search, and the type of drone surveillance technology utilized, an approach which I call the "Systematic Schematic of Differentiation." In short this principle entails that the form that regulations take ought to follow from the functions and objectives they are designed to serve and advance. Towards this end, I argue in (i)(a) that for persistent surveillance systems plenary permission should be granted to intelligence community subject to its fastidious observation of the "pure intelligence" rule (with a carve out exception for prosecution of terrorist and espionage activities). Conversely, for law enforcement officials, I propose that persistent-surveillance system's video feeds should be encrypted and accessible only after procuring a warrant based on probable cause.

For non-persistent surveillance drones I argue in (i)(b) that warrant requirements for areas plainly within the public view are ill-advised for both for law enforcement and intelligence officials alike. Rather they should be permitted plenary access to public areas on equal footing with any boy scouts or hobbyists yet subject to far more exacting scrutiny on the secondary uses towards which it is employed through an "Accountability Apparatus" governed by a (2) "Panoply of Protective Safeguards" including: (i) mandatory "intelligent" software; (ii) minimization protocols (iii) external, independent oversight; (iv) public notice and democratic control and (v) strict disciplinary sanctions and substantial civil remedies to enforce accountability. Lastly, for invasive searches involving areas not within the public view I propose

that traditional *ex ante* warrants based on probable cause should apply in keeping with the reasonableness requirement of the Fourth Amendment.

(i) *Wide-Area Persistent Surveillance Drones*

(a) Intelligence Community & The Pure Intelligence Rule

Several critically important distinctions must be made in the regulation of drone technology—foremost of which are the three "differentiation" principles I have articulated as part of my Systematic Schematic of Differentiation. These processes include distinguishing the *warrant protocols* of wide-area persistent surveillance systems (like the ARGUS-IV) from non-persistent surveillance drones, taking into account the *uses* towards which the information will be employed (i.e. the prevention of terrorism by the intelligence community vs. the prosecution of crime by law enforcement officials) and the location in which it takes place (public areas vs. private areas). This accords with the basic tenets of logic and reason, as different capabilities, purposes, and contexts call for differential regulation.[183]

The Supreme Court articulated precisely this kind of nuanced approach in its *Keith* opinion:

> We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.' The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crimes specified …Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some future crisis or emergency . . . Different standards may be compatible with the Fourth Amendment if

[183] As the founder and pioneer of the modern architecture, Louis Sullivan, famously noted about "form following function"—it appears to permeate nature itself: "Whether it be the sweeping eagle in his flight, or the open apple-blossom, the toiling work-horse, the blithe swan, the branching oak, the winding stream at its base, the drifting clouds, over all the coursing sun, form ever follows function, and this is the law. Where function does not change, form does not change. The granite rocks, the ever-brooding hills, remain for ages; the lightning lives, comes into shape, and dies, in a twinkling. It is the pervading law of all things organic and inorganic, of all things physical and metaphysical, of all things human and all things superhuman, of all true manifestations of the head, of the heart, of the soul, that the life is recognizable in its expression, that form ever follows function. This is the law." Louis H. Sullivan, *The Tall Office Building Artistically Considered*, Lippincott's Magazine, 403-409 (March 1896).

> they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.[184]

Yet, surprisingly few—if any regulation proposals to date—have attempted to meaningfully distinguish the two or propose a differential calculus with respect to either their use-limitations or procedural safeguards. I believe this is the single most important area for Congress and the Courts to recognize and will accordingly attempt to show why they are so demonstrably different and require regulations that are uniquely tailored to their particular capabilities and attributes.

Under a "smart" regulatory regime, Congress would recognize the unique needs of the intelligence community in prospectively gathering intelligence information to prevent the occurrence of disastrous events ranging from chemical, biological, and nuclear attacks to violent gun rampages like the two most recent ISIS attacks in Paris, France which claimed over a hundred and thirty lives and in San Barnardino, California where it is believed ISIS-affiliated operatives "massacred" 14 American citizens and left 17 more wounded.[185] In order to put the magnitude of these security threats into proper perspective, the New York Times recently found that from September 2014 to November 2015 ISIS has been responsible for "nearly 1,000 civilian deaths *outside* of Iraq and Syria."[186] Consequently, the need for the intelligence community to gain critical intel to thwart these nefarious plots has never been greater given the reality that we all now denizens in a new global epoch, the "Age of Terror."[187]

---

[184] United States v. U.S. District Court, 407 U.S. 297, 322-323 (1972).

[185] Rukmini Callimachi, *ISIS Claim Responsibility, Calling Paris Attacks 'First of Storm'*, New York Times (Nov. 14, 2015) http://www.nytimes.com/2015/11/15/world/europe/isis-claims-responsibility-for-paris-attacks-calling-them-miracles.html; Faith Karimi et. al, *San Barnardino Shooter 'Supporters' Of ISIS*, Terror Group Says, CNN News, (Dec. 5, 2015), http://www.cnn.com/2015/12/05/us/san-bernardino-shooting/.par

[186] Karen Yourish et al., *ISIS is likely Responsible for Nearly 1,000 Civilian Deaths Outside Iraq and Syria*, New York Times, (Nov. 17, 2015) http://www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html?_r=0

[187] See STROBE TALBOTT & NAYAN CHANDA, THE AGE OF TERROR: AMERICA AND THE WORLD AFTER SEPTEMBER 11, Yale Center for the Study of Globalization (eds. Talbott & Chanda 2002).

Moreover, as the ODNI General Counsel cogently explained in his plenary address on Privacy and National Security the needs of the intelligence community are quite distinct from those of other governmental entities:

> The business of … intelligence has always been fundamentally different from the business of criminal investigation. Rather than attempting to solve crimes that have happened already, we are trying to find out what is going to happen before it happens. [The intelligence community] may have only fragmentary information about someone who is plotting a terrorist attack, and need to find him and stop him. We may get information that is useless to us without a store of data to match it against … Or we may learn about a plot that we were previously unaware of, causing us to revisit old information and find connections that we didn't notice before—and that we would never know about if we hadn't collected the information and kept it for some period of time….[188]

Accordingly, Congress should authorize a "pure intelligence" rule for the intelligence community to conduct domestic drone surveillance activities which a clear prohibition on the use of evidence for criminal prosecutions except in circumstances involving terrorism, espionage or other similarly related matters of National Security. In this way, it will neither frustrate the efforts of intelligence officials in their effort to gain critical information germane to National Security nor resurrect the much maligned "wall" between the intelligence and law enforcement communities that many blamed for failing to prevent the 9/11 terrorist attacks.[189] Instead, it accords with sound reason and basic common sense—limiting the "uses" for which information collected can be lawfully applied to those particular areas of need where the intelligence

[188] Robert S. Litt, *Privacy, Technology and National Intelligence Collection*, An Address by General Counsel of the the Office of the Director of National Intelligence, (July 19, 2013) http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection

[189] *See* In re Sealed Case No. 02-001, 310 F. 3d. 717 n. 29 (FISA Ct. Rev. Nov. 18, 2002)(One agent, frustrated at encountering the "wall," wrote to headquarters: "[S]omeday someone will die--and wall or not--the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the National Security Law Unit will stand behind their decisions then, especially since the biggest threat to us now, [Osama Bin Laden], is getting the most 'protection.'").

community has a special and peculiar interests in discovering information *prior* to untoward event ever coming to pass.

(b) Law Enforcement Officials

Conversely, the needs of law enforcement officials pivot largely upon the prosecution of past crimes, rather than the prevention of future events. Accordingly, WAPS video feeds should be encrypted and accessible to law enforcement officials only *after* procuring a warrant based on probable cause *ex post*. That is to say, if police desire to gain access to the video recordings from WAPS surveillance repositories they must first obtain authorization from a detached and independent magistrate on the basis of probable cause in harmony with the letter and spirit of the Constitution. Additionally, lawmakers should be very weary of carving out any exceptions to this rule for emergency situations as this could lead to the very slippery slope that civil-liberties advocates fear most. Instead, regular non-persistent surveillance drones could easily fill in this gap under emergency circumstances and would likely achieve equal effectiveness (*see* section (ii) *infra*). Another bright line rule that would be wise for policymakers to adopt would be a strict felony requirement for WAPS surveillance requests. This would obviate the potential for targeting unpopular individuals or groups as well as prevent potential backlash from citizens who resent surveillance over trivial matters. Although, this rule may be under-inclusive since many crimes that do not qualify as felonies may be desirable to prosecute it would be a wise starting point so as to prevent backlash and opposition from overwhelming the support for the program and forestalling its successful enactment and implementation.

(ii) *Non-Persistent Surveillance Drones*

A different set of standards should apply for non-persistent surveillance drones. In short, broad discretion should be permitted for information collection in public places without any

requirement for obtaining a warrant, yet very strict requirements should be implemented for the aggregation, retention, dissemination, and downstream use of that information by law enforcement and intelligence officials. Given their less threatening capacity to collect, aggregate and synthesize our movement patterns, regulation of non-WAPS drones should instead focus on creating a panoply of protective mechanisms to constrain the misuse of information gathered that is unrelated to legitimate government inquiries.

2. The Accountability Apparatus: Implementing a Panoply of Protective Safeguards

In order for broad discretion to be granted for information collection by non-persistent surveillance drones there must be what I call a comprehensive "Accountability Apparatus" replete with a "Panoply of Protective Safeguards" to ensure that the use of drones always complies with the rules and protocol set forth by Congress and the Courts and accords with the fundamental values and principles of the American people. These protective safeguards would include: (i) mandatory "intelligent" software; (ii) minimization protocols (iii) external, independent oversight; (iv) public notice and democratic control and (v) strict disciplinary sanctions and substantial civil remedies to enforce accountability.

(i) *Mandatory "Intelligent" Software Programs*

Firstly, all government drones should come equipped with "intelligent software" to prevent the identities of individuals not part of the target search from being subject to gratuitous and offensive invasions of privacy. The first kind of "intelligent software" could be employed in several ways. For example, it could involve programing the system so that the video feed "automatically blur[s]" the faces of non-targeted individuals on adjacent properties thus reducing the risk of "unwanted observations of innocent people."[190] Additionally, it could employ

[190] McNeal, *supra* note, at 22.

software that limits the scope of view to the target area of inquiry with permission to expand the view subject to written justification which would then be noted in a data log and released to the general public (i.e. the expanded view request would be accessible *not* the video itself). A third possibility could include auto-blur technology for license-plates and addresses not subject to review. This could then be "unlocked" via a warrant if deemed germane to the investigation. These initial suggestions should not be construed as either comprehensive or exhaustive. On the contrary, this is an area ripe for innovative ideas and fresh, creative approaches to effectively balance the interests of privacy and security in new uncharted territory. Indeed, with the right combination of "intelligent" software protections in place, drones may someday soon actually provide *greater privacy protection* than manned aerial surveillance."[191]

(ii) *Minimization and Retention Protocols*

Secondly, minimization and retention protocols will likewise prove crucial to gain the approval of the public and limit the government's potential for abuse. Proper minimization protocol would require the automatic deletion of video surveillance taken after 180 days, unless the video was part of an on-going criminal investigation. This requirement would be imposed equally for law enforcement and intelligence officials alike for both wide-area persistent surveillance systems and non-persistent surveillance drones.

Some groups, however, object to this seemingly sensible 180-day limitation. The ACLU, for example, has proposed that Congress should restrict the retention of images of identifiable individuals captured by aerial surveillance technologies "unless there is reasonable suspicion that

[191] Gregory McNeal, *Drones and Aerial Survillance: Considerations for Legislators*, CENTER FOR TECHNOLOGY INNOVATION BROOKINGS INSTITUTE, 4 (Nov. 2014), http://www.brookings.edu/~/media/Research/Files/Reports/2014/10/drones-aerial-surveillance-legislators/Drones_Aerial_Surveillance_McNeal_FINAL.pdf?la=en.

the images contain evidence of criminal activity" or may be relevant to "an ongoing investigation or pending criminal trial."[192] Upon further reflection, however, several problems become evident with this approach which are not likewise present with a 180-day retention policy.

Firstly, the ACLU's strict requirement on retention is inconsistent with the currently accepted timeline mandated by the Presidential memorandum on UAVs which permits information retention for 180 days.[193] Secondly, it would undermine the ability of law enforcement officials to utilize video evidence for investigations that may develop a short while after the initial footage is captured yet may not qualify as an "ongoing investigation." Thirdly, it needlessly prevents storage of information on secure government servers that pose no threat of harm or injury to anyone (given that proper safeguards would be in place). Again, the storage of such information would do little to prevent or deter abuse but could in fact produce a great deal of harm to the government's ability to conduct legitimate inquiries into crime and terrorism. Instead, a reasonable time period like the 180 days mandated by the Presidential Memorandum would serve all these interests well without infringing upon the government's ability to carry out its duties and promote the public's safety.

(iii) *External, Independent Oversight*

Auditing by independent experts will also prove salutary to allay fears of abuse and ensure taxpayer funds are being well-spent. Towards this end, all regulation should include *ex-post* independent reviews for relevancy, accuracy of requests, bias-related targeting of particular

[192] Jay Stanley & Catherine Crump, Protecting Privacy From Aerial Survilance: Recommendations for Government Use of Drone Aircraft, American Civil Liberties Union (Dec. 2011), https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

[193] (with a few minor exceptions). *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552 (proposed Feb. 23, 2015) ("Information collected using UAS that may contain PII [personally identifiable information] shall not be retained *for more than 180 days* unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.").

individuals or groups, and other critical vetting mechanisms to mitigate the possibility of improper or abusive requests. This review could entail *ex post* judicial review by Article III judges or specially trained elected officials for political accountability, or administrative review from persons with the necessary qualifications, security clearances, training, background and expertise to handle delicate matters pertaining to national security and individual privacy. Another possibility could include the creation of a new venue analogous to the Foreign Intelligence Surveillance Court to facilitate expedited, specialized review. The Court could be called the Domestic Drone Surveillance Court or alternatively the National Security Administrative Court.

(iv) *Public Notice & Democratic Control*

In order for drone regulation to be effective it must also garner the respect and support of the people through various avenues of notification and responsiveness to democratic oversight, input, and control. Towards this end, the ACLU proposes that the government's policies and procedures for aerial surveillance technology should be "explicit and written, and should be subject to public review and comment."[194] Moreover, they propose that based upon this information subsequent policy decisions should be "democratically decided based on open information-not made on the fly" or by departmental "fiat."[195] Both proposals will prove salutary for a variety of reasons.

Firstly, public disclosure of policy will ensure accountability and transparency for as Justice Brandeis aptly noted long ago, "Sunlight . . . is the best of disinfectants."[196] That is to say,

[194] American Civil Liberties Union, Brief submitted to the Senate Jud. Comm. hearing on "The Future of Drones in America: Law Enforcement and Privacy Considerations," 11 (Mar. 20, 2013), http://www.judiciary.senate.gov/imo/media/doc/CHRG-113shrg81775.pdf.

[195] *Id.*

[196] Louis D. Brandeis, *Other People's Money and How the Bankers Use It,* Harpers Weekly, 92 (1914), http://www.law.louisville.edu/library/collections/brandeis/node/196.

both governmental officials and the general public alike will benefit from robust, respectful dialogue concerning the potential costs and benefits of the various policy choices before us. As a result of this rigorous vetting process, vague terms may become illumined by discussion, inefficient policies corrected, and ambiguous protocols prone to cause abuse may be amended under the influence of strong countervailing public opinion. Consequently, much will be gained but little lost by operating on the basis of clear and consistent policy guidelines that receive the overwhelming acceptance and approval of the people. More fundamentally, our nation was founded on the idea of a form of government in the words of Lincoln "*of*, *by*, and *for* the people" and this policy would accord appropriate weight to that founding principle. In other words, the drone policies that govern our domestic skies ought to reflect the values and commitments of the people and should be equally responsive to their censure through the implementation of corrective mechanisms build into the very architecture of the regulatory system itself. As one commentator has noted, "a healthy distrust of government is [about] as American as apple pie."[197]

Additionally, something similar to Professor McNeal's "transparency and accountability measures" for public notice would also be highly useful in furthering these democratic ends. McNeal proposes that drone usage logs should detail "who operated the system, when it was operated, where it was operated (including GPS coordinates), and what the law enforcement purpose for the operation was."[198] Additional he contends that flight logs should be made public to "allow privacy advocates and concerned citizens to closely monitor how aerial surveillance devices are being used, enabling the political process as a mechanism to hold operators

[197] Marc Jonathan Blitz et al., *Regulating Drones Under the First and Fourth Amendments*, 57 Wm. & MARY L. REV 49, 139 (2015).

[198] McNeal, *supra* note 118, 19-20.

accountable."[199] Finally, he notes that in circumstances where publishing usage logs "may reveal information that is law enforcement sensitive (such as an ongoing investigation) the agency operating the drone may keep their usage logs confidential until the investigation is closed."[200] These measures would likely prove highly useful for facilitating rigorous accountability and vetting of government activity and likewise garner broad and enthusiastic support lawmakers concerned with maintaining as much control over drone surveillance operations as possible.

(v) *Disciplinary Sanctions & Civil Remedies*

Disciplinary sanctions for government officials who fail to abide by the rules and regulations of drone surveillance will likewise prove crucial to the overall success of the program as well. That is to say, in order for the government to effectively implement a use-based approach to domestic drone surveillance regulation, civil remedies against the government must provide ample financial remuneration to incentivize citizens to hold the government accountable and strict disciplinary sanctions for government officials who violate these policies in order to disincentive officials from engaging in reckless, harmful, and abusive activities that injure the welfare of citizens and impugn the reputation of the government. Accordingly, vigorous enforcement will be critical to prevent governmental abuse, achieve optimal levels of data collection, and properly incentivize adherence to the rule of law. As Justice Brandeis rightly noted long ago:

> In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously … For good or for ill, it teaches the whole people by its example … If the Government becomes a lawbreaker, it breeds contempt for the law [and] invites every man to become a law unto himself.[201]

[199] McNeal, *supra* note 118, 19-20.
[200] McNeal, *supra* note 118, 19-20.
[201] Olmstead, v. United States, 277 U.S. 428 (Brandeis, J., dissenting).

3. Domestic Drone Surveillance Regulatory Synthesis

In sum, a targeted framework that follows a "Systematic Schematic of Differentiation" can achieve the interests of both security and privacy by creating a hybrid framework that meaningfully distinguishes the needs of the respective government agencies, differentiates public areas from private areas, and treats different drone capabilities differently. Moreover, by providing a robust "Accountability Apparatus" it will allow appropriate discretion to collect information pertinent to legitimate government inquiries but place sharp limits on the uses towards which that information can be applied with the full "Panoply of Protections" necessary to ensure the program's integrity and enduring success.

B. Tapping into the Power of Federalism: *Brandeisian* Laboratories of Experimentation

In order to gain the optimal level of benefits from drone technology and harness the full potential of our Federalist form of government, Congress would be wise to cautiously approach the regulation of drones so that it does not hinder or impede their evolution and development. Taking full advantage of the ability of States to experiment with drone regulation could provide a whole host of insights that would otherwise be unavailable if regulation were made in haste without considering all of the empirical data and evidence available to make informed and intelligent policy choices. As Professor Ryan Calo noted in his Congressional testimony, "Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose in the subsequence decade with advent of social networking and location based wireless services."[202]

[202] Ryan Calo, Brief to House Subcomm. On Crime, Terrorism, Homeland Security and Investigations, Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems, 5 (May 17, 2013), http://judiciary.house.gov/_cache/files/69365986-a0b1-4a21-ad9d-fc4e47762735/113-40-80977.pdf.

Consequently, Federal regulations should be particularly careful when implementing regulations in areas of rapid technological development like drones and proceed cautiously to benefit from the States ability to experiment with a variety of forms of regulation in this area. As Justice Brandeis famously explained *in New State Ice Co. v. Liebmann* it is the "happy incident" of federalism that States can function as "laboratories" to "try novel social and economic experiments without risk to the rest of the country."[203]

In other words, Brandeis argument highlights the fact that within our federalist system of distributed powers between the Federal Government and the separate States the whole country can benefit from harnessing the power of fifty autonomous state and local governments to test out various theories of privacy and acquire new measurable and quantifiable knowledge to improve, refine, alter, expand, or reject previously untested theories of privacy and put into practice what works. As one commentator has noted, as things currently stand, it will be particularly difficult for Congress to "design a preemptive, national-level policy" without first possessing more information about the particular type of drones that will be utilized and the privacy rules that will govern their use in the courts.[204] On the other hand, state regulation may very well yield the crucial insights necessary to strike the proper balance between privacy and security.[205]

Moreover, if states ambitiously experiment with drones the wealth of empirical data Congress will have at its disposal, will enable it to easily transition from conjectural speculation towards a more concrete, scientific understanding of the facts on the ground, and marshal those

[203] New State Ice Co. v. Liebmann, 285 U.S. 262 (1932).

[204] Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, The Brookings Institution (Sept 2014) http://www.brookings.edu/~/media/Research/Files/Reports/2014/09/civilian-drones-privacy/civilian_drones_privacy_bennett_NEW.pdf?la=en. See also Margot E. Kaminsky, Drone Federalism: Civilian Drones and th Things They Carry, 4 CAL. L. REV CIRCUIT 57 (May 2013) http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1007&context=clrcircuit.

[205] *Id.*

evidentiary findings to implement practices proven to be effective. Accordingly, if some states adopt more permissive regulations and other states adopt more restrictive regulations both instances would ultimately redound to the benefit of the Federal government by providing a wealth of information for emulation.

In conclusion, if the government were to adopt a hybrid regulatory approach carefully and narrowly tailored for the distinctive capabilities of different types of drones, the location of the search, and the different interests of law enforcement and intelligence officials that worked in conjunction with a federalist framework designed to cultivate the best practices from the various state "laboratories"—the government would be well on its way to creating an atmosphere primed to protect privacy and promote the public's safety with tested and proven results.

V.
RE-CONCEPTUALIZING PRIVACY LAW IN THE AGE OF DRONES, TWITTER, AND TERRORISM

At a time when the nation is called upon to give freely of life and treasure to defend and preserve the institutions of democracy and freedom, we should not permit any of the essentials of freedom to lose vitality through legal interpretations that are restrictive and inadequate for the period in which we live. – Justice Murphy[206]

Privacy, as we currently understand, it is now dead—or at the very least on critical life-support and in need of urgent care. In an age of drones, twitter, and terrorism a mere resuscitation of a dead and dying framework will simply not suffice. Instead a two-fold revolution must take place: first, a veritable privacy renaissance is needed to "restore our sense of injury" at a time when expectations of privacy are at an all time low and the protections afforded by the courts now rest on an increasingly narrow and thin foundation.[207] Secondly, new frameworks must emerge from the ashes and rubble of *Katz* to account for the radical threats posed by extremist terrorist groups bent on destroying the bonds that bind us all together as

[206] Goldman v. United States, 316 U.S. 129, 142 (1942) (J., Murphy, dissenting).
[207] *See* M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE (2011

Americans and fill our lives with bitterness, hatred, malice and fear. What we need is to transform of our mid-20th century model of privacy into a comprehensive 21st century model fit for the extraordinary times in which we live.

I contend that a use-based, mosaic theory of privacy will achieve precisely these objectives by producing a legal framework that is far more amenable to empirical evaluation and critique, better apt to ameliorate law enforcement efficiency and effectiveness, reduce the number of arbitrary and invasive governmental intrusions into our daily lives, and ultimately renew the spirit of America as a nation deeply and profoundly committed to protecting the principles of privacy and autonomy embodied in our Fourth Amendment.

A. Writing on the Wall: The Conceptually Bankruptcy of *Katz* and its Coming Demise

As Edward H. Levi famously noted in his classic book on 20th century jurisprudence—legal concepts tend to have a predictable shelf-life and follow a familiar three-fold cycle: creation, solidification, and breakdown.[208] At this third and final threshold scholars continue to pay it "lip service" and go to great pains to defend its continuing worth, yet the truth remains "it is useless" and has become nothing more than a "window dressing."[209] After following a well-tread path in the history of legal thought the *Katz* has finally reached this moment in its conceptual life and there is now a general consensus that it no longer serves as a meaningful check on governmental searches and seizures. After enduring a constant barrage of criticism for decades now it is at last primed to be supplanted by a new theory of privacy more in tune with the realities of modern times.

The proliferation of drones will likely catalyze *Katz's* demise and provide the long overdue coup de grâce to a dated and dying concept whose checkered chapter in the history of

[208] EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING, 10-11 (1949).
[209] *Id.*

American jurisprudence has at last reached its dénouement. In short, drones will expose *Katz's* conceptual bankruptcy for what it is—untenable in theory, unworkable in practice, self-defeating, fundamentally at variance with the core principles of our Constitution, and in dire need of relief from a new framework of privacy better equipped to meet the challenges of our time.

1. Untenable in Theory

Firstly, it should be noted that the major problem with *Katz* is not the court's inability to faithfully apply its content but rather with the conceptual bankruptcy of the *test itself*. As the *Kyllo* court rightly noted, "the *Katz* test … has often been criticized as circular, and hence subjective and unpredictable." It is circular in the words of Richard Posner because, "there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is."[210] Exasperated by this vapid tautology Posner wryly quipped, "these are threadbare arguments."[211]

2. Unworkable in Practice

The *Katz* test is also as the *Kyllo* court noted "subjective and unpredictable" because no matter how it is applied it is inconsistent with principles of jurisprudence that make the Court's judgment valid, binding, and legitimate. As Justices Scalia and Thomas have noted:

> those "actual (subjective) expectations of privacy that society is prepared to recognize as 'reasonable," bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable. When that self-indulgent test is employed … to determine whether a "search or seizure" within the meaning of the Constitution has occurred (as opposed to whether that "search or seizure" is an "unreasonable" one), it has no plausible foundation in the text of the Fourth Amendment.

[210] Richard Posner, *The Uncertain Protection of Privacy by the Supreme Court*, S. CT. REV. 173, 188 (1979).

[211] *Id*.

Nevertheless, the alternative is no better. That is to say, if the court were to reject importing its own preferences and instead faithfully apply the *Katz* test it would be forced into evaluating "contemporary community standards"[212] to determine social expectations and thus be reduced to the role of the Supreme "arbiter of [social] norms."[213] Thus, instead of adjudicating matters of Constitution law *qua* law, it would be forced to make decisions on nothing less than the vagaries of public opinion and in so doing gut the independence of the court, the integrity of its judgment, and the legitimacy of the law. In other words, no matter whether judges impose their own preferences or follow public opinion polls the inquiry itself it the problem as it adds unnecessary confusion and artificial speculation while simultaneously obscuring the primary objective—the protection of privacy. Accordingly, the real problem is not the Constitutional text, but rather the *Katz* test *itself*.

3. The Downward Spiral of Self-Defeating Expectations

Moreover, even if one were too look past these issues, generations of continued erosions of privacy have led to a self-defeating process of degraded expectations that in turn further generate and perpetuate the decline of expectations and the deprivation of privacy. As Justice Alito noted in his *Jones* concurrence:

> The *Katz* test rests on the assumption that [a] hypothetical reasonable person has a well developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.

[212] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 851 (2002).
[213] *Id.*

Moreover, in addition to erosion from institutional actors like Google, Twitter, and Facebook compromising our "transactional privacy" the legal test itself may function to further erode those expectations as well—for as Erwin Chemerisky ironically noted, the government "can deny privacy just by letting people know in advance not to expect any."[214] That is to say, as individuals "internalize each incremental encroachment" and those encroachment in turn are *validated by the courts* this drives a vicious "downward spiral" of expectations because its narrow focus on the current level of expectations perpetuates the cumulative "incremental erosion of privacy" that guts and degrades privacy still further.[215] Consequently, "without some structural changes to restore the balance, the erosion of privacy may be a foregone conclusion."[216] That is to say, without a new system in place to restore robust expectations of privacy the entire project of measuring expectations by current expectations becomes an entirely self-defeating process.

4. Fundamentally at Variance with Our Most Foundational Constitutional Principle

Most devastating of all, it is strikingly at variance with our the most foundational principle of our Constitution—namely that no fundamental right should ever turn upon the vagaries of the ballot box nor depend on the court of public opinion for its legitimacy.[217] That is so say, public consensus "has no standing from a normative viewpoint when *fundamental rights* are at stake."[218] As one commentator has cogently noted:

---

[214] Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L. J. 643, 950, (2007).

[215] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 845 (2002).

[216] *Id.*

[217] As Anthony G. Amsterdam notes the "actual, subjective expectation of privacy . . . can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection." Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

[218] Amitai Etznioni, *Essay: Eight Nails into Katz's Coffin*, 65 CASE WESTERN RESERVE L. REV. 413, 416 (2014).

> If an overwhelming majority of Americans agrees … that "fishing expeditions" by the police are fully acceptable because "those who did nothing wrong have nothing to hide," this does not mean that a court should accept this consensus and allow it to trump the court's judgment as to what the Constitution entails and what is just and right. In short, from a normative viewpoint, the expectation of the public as to what and who may or may not be searched should matter little.[219]

This is quite simply the bedrock principle of our liberal democracy for as Justice Jackson famous declared: "The very purpose of a Bill of Rights was to withdraw certain subjects from the vicissitudes of political controversy, to place them beyond the reach of majorities and officials and to establish them as legal principles to be applied by the courts."[220] Accordingly, it is the emphatically province and duty of the courts to defend our most fundamental rights to the uttermost—*irrespective* of any "societal expectations of privacy" to contrary—and no principle of law that contradicts that foundational principle ought to govern our courts much less diminish our most cherished constitutional liberty *one single iota*. "If there is any fixed star in our constitutional constellation it is this—one's right to life, liberty, and property …. and other fundamental rights may not be submitted to [a] vote."[221]

Consequently, the rationale for *Katz* appears to break down on several levels and makes the constitutional inquiry into privacy a far less "reliable, trustworthy [and] independent criterion" than ought to be permitted for determining one of our nation's most precious and fundamental liberties—the right to be free from arbitrary and capricious governmental intrusion.[222]

---

[219] *Id*.
[219] EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING, 10-11 (1949).
[220] West Virginia State Board of Education v. Barnette, 319 U.S. 624, 639 (1943).
[221] *Id*. at 639.
[222] Amitai Etznioni, *Essay: Eight Nails into Katz's Coffin*, 65 CASE WESTERN RESERVE L. REV. 413, 416 (2014).

Thus, after conducting a thorough and complete analysis of the *Katz* test and examining its underlying principles one is forced to draw the conclusion that it is a wholly inadequate paradigm of privacy, sapped of all vitality, and broken beyond all semblance of repair. Consequently, the Court would be well-advised to discard its circular, self-defeating inquiry into sorting out *what a judge thinks society thinks* altogether and instead implement specific, meaningful categories of privacy protection capable of achieving clarity, consistency, and predictability for citizens and government officials alike. I believe that a use-based, mosaic theory of privacy will achieve precisely these ends by expanding the breath and depth of coverage, building greater consistency and predictability into the court's analysis, and establishing clear principles of law.

B. Towards a Use-Based, Mosaic Theory of Privacy

(i) Mosaic Theory

As drones loom large on the horizon, the time has come to revolutionize our privacy jurisprudence and breath new life into the Fourth Amendment. In place of the antiquated *Katz* test, the court should adopt a two-fold framework that first recognizes that privacy is not spatially or temporally bound and secondly as a corollary of that principle recognizes the that protection of the "indefeasible right to personal security and personal liberty"[223] embodied in our Fourth Amendment must necessarily expand its protections to defend citizens' rights in the digital age to be free from from arbitrary and invasive intrusions into the most intimate details of their lives—*whenever and wherever they are imperiled*. [224]

[223] Boyd. V. United States 116. U.S. 616, 630 (1886).
[224] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).

The upshot of these two principles is that privacy can no longer seen in terms of a particular moment in time or as merely an isolated piece of data abstracted from the larger web of human experience that now constitutes identity in a modern age of information. As Judge Leon noted in the landmark meta-data case "unique privacy interests" are implicated by the "long-term storage" of information and accordingly "records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[225] In other words, "technology" can now yield with "breathtaking quality and quantity" a highly detailed portrait of our lives—"not simply of where we go, but by easy inference, our associations—political, religious, amicable [as well as] amorous."[226] Consequently, "Just as a search of a house requires probable cause even when the occupant is not at home, the government should have to justify privacy-invading virtual searches even though no physical confrontation is involved."[227]

The court easily can integrate this into its jurisprudence by recognizing that the acquisition of information may under certain circumstances constitute a "seizure" within the meaning of the Fourth Amendment when its uses are deemed "unreasonable." In other words, after the surveillance has been conducted—the aggregation,[228] use,[229] and retention[230] of that data can and must implicate reasonableness scrutiny pursuant to the Constitution's protection of

[225] Klayman v. Obama, 957 F. Supp. 2d 1, 35-36 (D.D.C. 2013).

[226] Christopher Slobogin, *Is the Fourth Amendment Relevant*, in CONSTITUTION 3.0, 22 (eds. Jeffrey Rosen & Benjamin Wittes 2011).

[227] *Id*. at 23.

[228] Aggregation is the "gathering of information about a person whether from one or multiple sources." Thompson, *supra* note 33, at at 9. The privacy theory of aggregation supposed that "while the collection of bits of data about a person may not violate his or her privacy interests, extensive collection of information about him or her can rise to the level of a legal privacy intrusion." *Id.*

[229] Improper use of data entails "data collected for an authorized purpose, but subsequently used in an unauthorized way." *Id.* at 10. Instead of focusing on requiring warrant before they are operated, policymakers should instead "regulate how that information is used." *Id.* at 10.

[230] Retention of data is an increasing concern given the near "limitless ability of the government … to store and retain information about individuals." *Id*. at 10.

"persons"—in the most full and meaningful sense of the word—guaranteed by the Fourth Amendment. Hence, the acquisition of information would not be viewed in isolation—but as part of a tapestry and web of human life—and justly accorded the proper protection it deserves.

As Professor Harold Krent has persuasively argued, "Control over private information is one of the most fundamental attributes of any notion of privacy, and although privacy may not be the only value underlying the Fourth Amendment, it should continue to play a pivotal role in shaping search and seizure doctrine."[231]

Fortunately, the Court has recently awakened to this new reality and took a step in the right direction by recognizing a more limited version of the use-based, mosaic theory of privacy advocated in this article in their 2014 decision in *Riley*.[232] The Court unanimously stated:

> 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." The fact that technology now allows an individual to carry such information in his hand does not make the information *any less worthy of the protection for which the Founders fought*.[233]

Accordingly, in place of the crusty old property-based model of privacy and the self-defeating expectations offered by *Katz*, searches and seizures must now moving forward be construed to protect invasions of privacy that take place over a long periods of time and even downstream as they perforce implicate the scrutiny of reasonableness demanded by our Constitution's Fourth Amendment. In place of the confusion caused by *Katz's* obfuscation of privacy, in this new epoch of jurisprudence the court will instead go to the heart of the matter itself to determine whether the government's use of information constitutes a privacy invasion on

[231] *Id.*
[232] Riley v. California, 134, S. Ct. 2473 (2014)
[233] *Id.* at 2491(emphasis added).

its merits—as unreasonable, invasive, and contrary to the dictates of privacy embodied in our Constitutional heritage.

Finally, in clearing out the cobwebs of *Olmstead* and *Katz*, we would be well-advised to re-open the books of *Boyd*—the landmark Fourth Amendment case of the 19th century—and internalize its bold and vivacious message:

> The principles laid down [in the Fourth Amendment] affect the very essence of constitutional liberty and security … they apply to all invasions on the part of the government … of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security and personal liberty…[234]

Thus, heeding the spirit of the Constitution and the precedents of the court construed in the best possible light we should recognize that if the Fourth Amendment truly protects "people, not places," then the time has come for the Court to at last put that Constitutional principle into practice.[235]

(ii) Use-Based Theory of Privacy

For far too long privacy-advocates, Congress, and the Courts have concentrated their attention on the wrong issues for privacy protection, focusing on the collection of information, rather than its use. Granted, the government cannot use information if it doesn't have it in the first place. Nevertheless, the government already routinely collects extraordinary amounts of information and there is little reason to believe that it will not continue to do so with the threat of terrorism and mass-violence becoming more and more prevalent and pervasive with each passing

[234] Boyd. V. United States 116. U.S. 616, 630 (1886).

[235] As one commentator concluded, "Katz is either a convenient fiction or a serious violation of the most basic principles of our polity and should be allowed to expire, the sooner the better." Amitai Etznioni, *Essay: Eight Nails into Katz's Coffin*, 65 CASE WESTERN RESERVE L. REV. 413, 416 (2014).

day.[236] Instead of attempting the herculean task of turning back the hands of time or reversing the rotation of the earth, privacy advocates would be much better served investing their time, energy and efforts in controlling what the government *does* with information after its gathers it since the latter "may now threaten privacy more than the collection itself.[237] That is to say, the narrow focus on information collection to date by privacy advocates must be recognized for what it is—terribly misguided.

Instead of focusing on requiring warrants before drones are operated policymakers should instead direct their attention towards permissible and prohibited uses to prevent even the very possibility of misuse. Funneling information towards only expressly recognized and permissible uses would provide a far more sensible framework for regulation since it would provide the same degree of control of the "effects" of drones, yet permit much more latitude for beneficial use. From taxpayer savings, to finding lost children, to deterring crime, to overseeing the borders, to aiding overworked, understaffed and underfunded police agencies, to monitoring environmental safety and natural disasters the potential applications of drone technology to enhance and uplift the welfare of society is truly limitless.

Accordingly in order to gain the full benefits of harnessing their power we must allow for greater latitude at the first stage of data collection and then focus our attention on constructing "rules that strictly regulate what the government can do with [that] information."[238] Moreover,

---

[236] *See* Rukmini Callimachi, *ISIS Claim Responsibility, Calling Paris Attacks 'First of Storm'*, New York Times (Nov. 14, 2015) http://www.nytimes.com/2015/11/15/world/europe/isis-claims-responsibility-for-paris-attacks-calling-them-miracles.html; *See also* Faith Karimi et. al, San Barnardino Shooter 'Supporters' Of ISIS, Terror Group Says, CNN News, (Dec. 5, 2015), http://www.cnn.com/2015/12/05/us/san-bernardino-shooting/.par. *See also* Karen Yourish et al., *ISIS is likely Responsible for Nearly 1,000 Civilian Deaths Outside Iraq and Syria*, New York Times, (Nov. 17, 2015) http://www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html?_r=0

[237] Harold Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995).

[238] Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, in in CONSTITUTION 3.0, 39 (eds. Jeffrey Rosen & Benjamin Wittes 2011).

we must recognize that "data manipulation can have an amplifying effect" that turns low-impact information in isolation into "high-impact information when processed."[239] Consequently, in order to reap the full benefit of this process we ought to "allow the initial collection of information" but then "place sharp limits on the later stages" of its "processing, use and disclosure."[240]This will necessarily entail an adjustment in our mindset, evaluative practices, and overall adjudicatory framework regarding what constitutes an invasion of privacy and a new methodology for assessing whether an that invasion has occurred *vel non*.

In sum, I believe that a use-based, mosaic framework of privacy working in concert with "smart" regulations will provide the necessary clarity and consistency to establish resilient protections and effective limitations that can be practically implemented, adequately supervised, and democratically controlled. If appropriately fashioned this combination of protections could go a long way in ensuring that our security and our privacy are strengthened and preserved as we move forward into a brave new world full of tremendous *promise* and *peril*.

[239] *Id*. at 43-44.
[240] *Id.*

CONCLUSION

As the power and influence of drone technology continues to expand and ascend to new heights, dramatic and far-reaching decisions will have to be made by our judges and lawmakers to determine nothing less than the fate and destiny of our American way of life. With our most cherished values and the very character of our nation hanging in the balance, the time has come to act firmly and decisively to revolutionize our laws and renew the spirit of America as a nation deeply and profoundly committed to protecting the principles of privacy embodied in our Fourth Amendment.

Towards these ends, I have argued that the court should not merely tinker within existing bounds of the *Katz* privacy test, but instead revolutionize the framework from the bottom-up with a fresh, new perspective predicated upon the "*uses*" towards which the acquired information is to be employed and a *reasonableness* analysis that recognizes the new reality of the digital age—that information does not exist in a vacuum but when gathered, organized and assembled in place becomes a *mosaic*—depicting the narrative and identity of a unique human life and experience. Walking in the park, to the bar, to see one's doctor or go to one's place of worship are not individually matters of privacy concern *per se*. But when these isolated comings and goings are collated and used to incriminate, intimidate, or embarrass they are no longer within the province of the public domain but are now enveloped in the broader umbrella of 21st century privacy protections—not merely on the basis of a *physical trespass* being triggered nor by divining a particular individuals expectation of privacy—but instead on the basis of its violation of a right more fundamental than the isolated travel patterns connote—the *Brandeisian* right to be "left alone." [241]

[241] *See* Olmstead, 277 U.S. at 478 (Brandeis, dissenting) ("The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of

The currently haphazard, piecemeal legislation governing the activity of drones is woefully inadequate to meet the task before us. Though the law is ill-equipped at the moment, with strong leadership and a sound strategy we can face these challenges with success—without the high risk attendant to either hastily responding to the next great national emergency, or even worse—purposively waiting for such an emergency to compel us to act. Instead, we can and must address the future use of drones proactively by grappling with this coming storm head-on in the present—recognizing its significance as the preeminent national security issue of our time.

There can be little doubt that the stakes are high and the margin for error is slim. Carefulness and caution ought to be our guiding lights to be sure. But these prudential constraints should not be blind us to our history and our heritage as Americans. Timidity and fearfulness have never suited the blazing spirit of American exploration. From the wild trails of Lewis and Clark's Great Expedition, to the sandy beaches of the Wright Brothers first flight, to the innovative assembly lines of Ford's model T, to Armstrong's triumphant march upon the moon—Americans have always been pioneers blazing new trails and exploring new frontiers. Drones *are* the next frontier, the only question that remains is *how will we respond to the challenge*?

---

his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, *the right to be let alone* -- the most comprehensive of rights and the right most valued by civilized men.).