PREVENTING AN AIR PANOPTICON: A PROPOSAL FOR REASONABLE LEGAL RESTRICTIONS ON AERIAL SURVEILLANCE

Jake Laperruque *

INTRODUCTION

Imagine a world where a small plane flies miles above a city, effectively invisible to its inhabitants, but looking down on them. Meanwhile, a series of drones, controlled in a semi-automated pattern by a single operator, hover over the surrounding suburbs. A select group of monitors—no more than a dozen members of the local police force—pinpoint areas of interest in real time, including a large protest, several doctors' and lawyers' offices, and a mosque. These officers are able to zoom in from cameras on the high-flying aircraft to identify individuals by their faces and log their activities. Meanwhile, a small group of federal agents review footage from these planes recorded over the course of the last sixth months, creating a precise map of the movements of hundreds of "persons of interest" over that entire period, and cataloging the places they visited and people they interacted with. Using automated identification tools, this process is rapid and simple. The agents will soon move on to a new set of targets, ensuring the government has a complete movement log of a huge portion of the metro area's population in time to repeat the process for the next six-month period.

To avoid living in a society with this "Air Panopticon," we cannot continue to rely on the limits of technology—the only shield we may possess is the limit the law places on pervasive and unrestricted surveillance from the sky. Many technologies are upending how we view surveillance and the limits the Fourth Amendment places on it in maintenance of a democratic society. The Supreme Court has recognized this issue with regard to particu-

* Senior Counsel, The Constitution Project, Washington, D.C. J.D., 2013, Harvard Law School; B.S., 2010, Washington University in St. Louis.

lar technologies; however, we must also do so with more general surveillance techniques.

This article highlights the growing risk of one technique in particular—modern aerial surveillance—and discusses how we might respond. First, this article describes the growing power of aerial surveillance, focusing on both new and evolving technologies. Second, it examines the unique features and risks to privacy that aerial surveillance poses. Third, it highlights the potential abuses to which this technology could lead to. Fourth, it reviews the existing legal standards for aerial surveillance, and proposes a new rule to reasonably limit the scope of aerial surveillance.

I. THE GROWING POWER OF AERIAL SURVEILLANCE

Aerial surveillance is not a new phenomenon. It was first employed for military reconnaissance using hot air balloons by the French army in 1794. United States law enforcement aerial surveillance has existed since the 1920s.[1] However, due to a variety of new and evolving technologies, aerial surveillance is rapidly advancing, offering the government unprecedented power.

A. *New Technologies*

The new aerial surveillance technology that has garnered the most public attention is unmanned aerial vehicles, commonly called drones. Since their deployment as combat aircraft more than a decade ago, drones have developed to serve a variety of purposes, including domestic aerial surveillance.[2] A significant number of drones are already deployed by federal, state, and local law enforcement for domestic surveillance.[3]

1. ARNOLD E. VAN BEVERHOUDT, JR., THESE ARE THE VOYAGES: A HISTORY OF THE SHIPS, AIRCRAFT, AND SPACECRAFT NAMED ENTERPRISE 115 (2d ed. 2013); *see also Fixed Wing Aircraft in Law Enforcement*, LAW OFFICER (Jan. 3, 2009), http://lawofficer.com/archive/fixed-wing-aircraft-in-law-enforcement/.

2. *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking*, ELECTRONIC PRIVACY INFO. CTR. (Aug. 2005), http://www.epic.org/privacy/surveillance/spotlight/0805/.

3. Conor Friedersdorf, *The Rapid Rise of Federal Surveillance Drones Over America*, THE ATLANTIC (Mar. 10, 2016), http://www.theatlantic.com/politics/archive/2016/03/the-rapid-rise-of-federal-surveillance-drones-over-america/473136/; *see also Surveillance Drones*, ELECTRONIC FRONTIER FOUND. (July 12, 2016), https://www.eff.org/issues/surveillance-drones.

Additionally, military-grade aerial surveillance technologies have developed for law enforcement use. In January 2016, the city of Baltimore began a citywide aerial surveillance program managed by a private firm using Cessna planes.[4] This firm, Persistent Surveillance, began operating this urban aerial surveillance to aid the American military in Iraq.[5] The Cessna planes, flying at a height of roughly 8500 feet, would watch over "an area of roughly 30 square miles and continuously transmit[] real-time images to analysts on the ground."[6] Analysts could request that the planes focus in on specific locations or events, and footage from the planes could then facilitate real-time tracking from the air.[7]

Persistent Surveillance adapted as a security vendor to serve in a law enforcement function and, via an anonymous grant, was funded to begin surveillance operations over Baltimore.[8] The program is capable of monitoring virtually the entire city, and in response to requests, it can hone in on a particular area as narrow as a street corner.[9] Even without a full zoom capable of visual identification, once a target is identified, the aircraft's camera can follow the path of the particular individual in low resolution, permitting Baltimore police to easily engage in long-term location tracking.[10]

While the managers of the program insist that it is only used to track active suspects, there is no independent oversight or restrictions limiting whom the police can target with this program.[11] The public was not made aware of the program until August of 2016, and even Baltimore's mayor was not notified of its existence

4. Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.

5. *Id*.

6. *Id*.

7. *Id*.

8. *Id*.

9. *See id*. ("Analysts on the ground could see individual cars moving through the streets.").

10. Kevin Rector, *Baltimore Surveillance Flight Data Suggest Homicides, Shootings Were Captured*, BALT. SUN (Oct. 7, 2016), http://www.baltimoresun.com/news/maryland/investigations/bs-md-sun-investigates-surveillance-dates-20161007-story.html ("The cameras do not provide high-resolution images, but allow for analysts—employed by the program's private operator, Persistent Surveillance Systems—to track individuals and vehicles coming into and leaving crime scenes. If the plane was filming a certain location at the time a shooting occurred, the analysts could go back in time to track any identified suspects through the city.").

11. *See* Reel, *supra* note 4.

prior to deployment.[12] Persistent Surveillance hopes the program in Baltimore will serve as a model that will be employed in cities throughout the country in the future.[13]

B. *Evolving Technologies*

In addition to the development and deployment of new technologies for aerial surveillance, evolving technologies present serious concerns for the future.

1. Drones

One key area of evolving technology is drones. Drones are advancing in two key ways with ramifications for privacy rights. First, drones are constantly decreasing in size.[14] Civilian engineers and the military are both developing micro-drones that resemble flying insects, such as the penny-sized "RoboBees" in development at Harvard.[15] In time, these incredibly small drones will be capable of longer flight and surveillance.[16] When their size is reduced, drones become more maneuverable and less detectable.[17] These features will facilitate greater surveillance capabilities—miniature drones will be able to go into narrow areas not

12. *See* Kevin Rector & Luke Broadwater, *Report of Secret Aerial Surveillance by Baltimore Police Prompts Questions, Outrage*, BALT. SUN (Aug. 24, 2016), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-secret-surveillance-20160824-story.html.

13. *See* Reel, *supra* note 4 ("By 2012, McNutt was approaching the police departments of the 20 most crime-ridden jurisdictions in the country, marketing his services.").

14. Jesse Young, *Police Department Drone Use: Potential and Risks*, DRONEGURU (Mar. 14, 2015), http://www.droneguru.net/police-department-drone-use-potential-and-risks/.

15. *See Autonomous Flying Microbots (Robobees)*, WYSS INST., https://wyss.harvard.edu/technology/autonomous-flying-microbots-robobees/ (last visited Feb. 17, 2017); Conor Friedersdorf, *Like a Swarm of Lethal Bugs: The Most Terrifying Drone Video Yet*, THE ATLANTIC (Feb. 19, 2013), http://www.theatlantic.com/technology/archive/2013/02/like-a-swarm-of-lethal-bugs-the-most-terrifying-drone-video-yet/273270/ ("An Air Force simulation says researchers are at work on killer robots so tiny that a group of them could blend into a cityscape."); Michael Zhang, *The $40,000 'Bug' Camera Drone Being Tested by the US Military*, PETAPIXEL (Dec. 7, 2015), http://petapixel.com/2015/12/07/the-40000-bug-camera-drone-being-tested-by-the-us-military/.

16. *See* Kris Osborn, *Air Force Chief Scientist: Future Drones Stealthier—More Autonomous*, DEF. SYS. (Oct. 10, 2016), https://defensesystems.com/Articles/2016/10/10/Future-Drones.aspx?Page=1; *see also* Robert Beckhusen, *The Army's Newest Drone Can Stay Airborne Forever: PARC Floats Above Infantry Bases—Provided There's Power Down Below*, WAR IS BORING (Jul. 24, 2014), https://warisboring.com/the-armys-newest-drone-can-stay-airborne-forever-384c2d5e6706#.76ox535ae.

17. Osborn, *supra* note 16.

accessible to current aircraft.[18] In terms of detectability, such drones will become ever-more inconspicuous; future devices could potentially hover outside a window or in an individual's yard absent any notice.

Second, drones are developing "swarm capabilities," meaning a single human pilot is able to simultaneously control multiple drones.[19] The military is developing drones with swarm capabilities, called "LOw-Cost Unmanned aerial vehicle Swarming Technology" ("LOCUST"), with the goal of a single pilot controlling many low-cost swarming aircrafts for enemy anti-air defenses to destroy.[20] If swarm capabilities become common and are incorporated into law enforcement's use of drones in the future, it will reduce resources needed to manage these devices, and thereby increase the government's surveillance capabilities. Whereas a fleet of pilots might be needed today, in the future a single officer could control enough drones to cover an entire metro area and outlying suburbs.

2. Photo Zoom and Resolution

Another critical area of evolving technologies in aerial surveillance is photo zoom and resolution. Photo zoom and resolution are advancing in a manner that gives aerial surveillance unprecedented power in terms of identification.[21]

18. *See id*. (explaining how swarms of drones could overwhelm enemy detection measures); *see also* George Leopold, *DoD Ramps Micro-Drones after Successful 'Swarm' Test*, DEF. SYS. (Jan. 13, 2017), https://defensesystems.com/articles/2017/01/13/swarmleopold.aspx (noting that current Perdix mini-drones have a wingspan of just 11.8 inches).

19. Osborn, *supra* note 16.

20. Kelsey D. Atherton, *LOCUST Launcher Fires a Swarm of Navy Drones*, POPULAR SCI. (May 24, 2016), http://www.popsci.com/navys-locust-launcher-fires-swarm-drones.

21. *See, e.g.*, Sebastian Anthony, *DARPA Shows Off 1.8-Gigapixel Surveillance Drone, Can Spot a Terrorist from 20,000 Feet*, EXTREMETECH (Jan. 28, 2013), https://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet.

One example of this growing power is the Aeryon HDZoom30. This high-resolution camera was developed in 2015.[22] It is currently recommended for law enforcement and commercial uses, at a cost that makes it a viable, though not readily accessible, investment for many police departments.[23] The Aeryon HDZoom30 has the capability to zoom in and achieve a precise visual identification from 1000 feet.[24] From this distance, it is capable of taking photo and video that can zoom in to a range that can read a license plate or recognizably view an individual's face.[25]

1.a

1.b

1.c

Figure 1: Images from an Aeryon HDZoom30 product demonstration video. Image 1.a. is a still image from a film of a set of cars from a distance of 1000 feet, with the camera not zoomed in. Image 1.b. is the camera zoomed to a magnification capable of reading the license plates on the cars. Image 1.c. is the camera zoomed to a magnification capable of identifying the faces of individuals standing next to the cars.[26]

22. Press Release, Aeryon Labs Inc., Aeryon Labs Introduces the Aeryon HDZoom30 Imaging Payload, Enabling Aerial Image Capture at 30x Optical Zoom (Feb. 23, 2015) [hereinafter Aeryon Labs Introduces the Aeryon HDZoom30 Imaging Payload], http://www.aeryon.com/press-releases/aeryon-labs-introduces-the-aeryon-hdzoom30-imaging-payload-enabling-aerial-image-capture-at-30x-optical-zoom.

23. *Aeryon HDZoom30 Imaging Payload*, AERYON LABS INC., https://www.aeryon.com/aeryon-hdzoom30 (last visited Feb. 17, 2017). The precise cost of the Aeryon HDZoom30 remains confidential. *See* David Ponce, *Aeryon HDZoom30 Camera Can be Mounted on a Drone, Spots Faces From 1000 ft. Away,* OH GIZMO (Mar. 3, 2015), http://www.ohgi2Mo.com/2015/03/03/aeryon-hdoom30-camera-can0be-mounted-on-a-drone-spots-faces-from-1000-ft-away/.

24. Aeryon Labs Introduces the Aeryon HDZoom30 Imaging Payload, *supra* note 22.

25. *Id.*

26. Aeryonlabs, *Aeryon HDZoom30 Imaging Payload*, YOUTUBE (Feb. 23, 2015), https://www.youtube.com/watch?v=LF-cDP04JaA.

A low flying aircraft or drone could use this type of camera not only to observe an area, but also to identify individuals at an event or location, log their activities, and track them.

However, the most ominous photo resolution aerial surveillance technologies are not those that are available to law enforcement in limited circumstances, but rather what will soon be available to the general public. The most prominent example of this point is the Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System ("ARGUS-IS"). The ARGUS-IS is a video recording technology developed by Defense Advanced Research Projects Agency ("DARPA"), the Department of Defense agency tasked with developing new and innovative technologies for military use.[27]

The ARGUS-IS is an entirely different class than high-resolution and zoom cameras such as the Aeryon HDZoom30. The ARGUS-IS "can resolve details as small as six inches from an altitude of 20,000 feet."[28] The field of view obtained by this device is immense; at full altitude it can cover an area of ten square miles, roughly half the size of Manhattan, with full precision.[29]

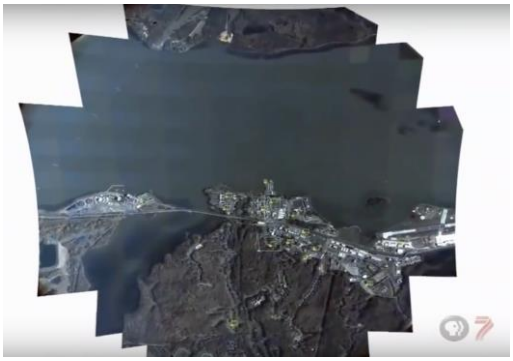
It is critical to note that this is not a zoom function where the field of view is narrowed to obtain precision. With the ARGUS-IS, the resolution is so strong that this extreme level of magnification exists *continuously throughout the entire field* from the far-off 20,000-foot distance; this means that no zoom and corresponding loss of field of view is required to obtain this extreme degree of intimate monitoring.[30]

27. *See* DEF. ADVANCED RESEARCH PROJECTS AGENCY, BREAKTHROUGH TECHNOLOGIES FOR NATIONAL SECURITY 26 (Mar. 2015), http://search.darpa.mil/viewer/index.jsp?start=0&proxy=%2F&sessionid=86dfde70-5dc6-4288-acaf-14afa306f20a.

28. Anthony, *supra* note 21.

29. *Id.*

30. *Id.* ("With an imaging unit that totals 1.8 billion pixels, ARGUS captures video (12 fps) that is detailed enough to pick out birds flying through the sky, or a lost toddler wandering around. . . . The end result . . . is a mosaic that can be arbitrarily zoomed. In the video, a[n] engineer zooms in from 17,500 feet to show a man standing in a parking lot doing some exercises.").

2.a 

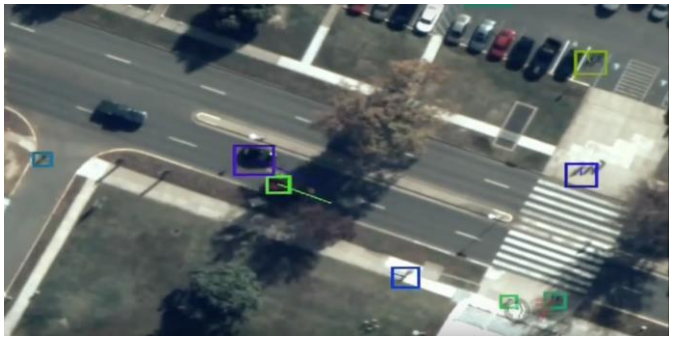
2.b 

Figure 2: Still shots of the video filmed from ARGUS-IS. Image 2.a. shows the human-eye view from the ARGUS-IS at 17,500 feet, while Image 2.b. shows the ability of the ARGUS-IS to provide an accurate view of a street-level image at any point within the field, solely via its resolution and without a zoom that narrows the field.[31]

In terms of surveillance, the implications of this development are profound. Multiple monitors could zoom in on numerous points simultaneously, regarding—with resolution for precise viewing—events occurring miles apart. Alternatively, the ARGUS-IS could record a wide field for a prolonged time, and monitors could later zoom in on this recorded material, with extreme precision, on any spot within the field.

If law enforcement possessed the ARGUS-IS or equivalent technology, it could equip an aircraft with that technology, fly it

31. FreakyVidsDaily, *1.8 Gigapixel ARGUS-IS. World's Highest Resolution Video Surveillance Platform By DARPA*, YOUTUBE (Jan. 27, 2013), https://www.youtube.com/watch?v=QGxNyaXfJsA ("This whole image is at a very, very fine resolution, so if we wanted to know what is going on in any spot along this image, say near this building at this intersection, we can generate a moving image, that shows what's going on in the area.").

at a high altitude of 20,000 feet, and record an entire urban area.[32] It could then zoom in to specific locations—a street corner, office entrance, crime scene, meeting of interest, public demonstration, or home—and identify individuals. It could track identified individuals as they traverse a city, log visits, or interact with others. The ARGUS-IS took thirty months and cost $18.5 million to develop, but the costs and capabilities for replication and deployment are unknown.[33]

If the ARGUS-IS or equivalent photo resolution technology becomes standard issue for law enforcement aerial surveillance, it will mark the end of anonymity.

To his credit, Persistent Surveillance CEO, Ross McNutt, has insisted he will not allow his program to be used in such an invasive manner. "Even as the technology advances and the camera lenses continue to get more powerful, he says, his company will choose to widen its viewing area beyond the current 30 square miles rather than sharpen the image resolution."[34] However, the fact that "[h]e's exasperated when his system is criticized not for what it does, but for its potential"[35] seems unfairly dismissive of the system's risks. Persistent Surveillance has set the precedent, and even if this company is unwilling to augment its capabilities, surely others will.

32. Current rules already permit the FBI to monitor entire neighborhoods or communities at an extremely low standard of suspicion, and these standards could be internally rolled back to permit even more pervasive surveillance. *See* Cora Currier, *Based on a Vague Tip the Feds Can Surveil Anyone*, THE INTERCEPT (Jan. 31, 2017), https://theintercept.com/2017/01/31/based-on-a-vague-tip-the-feds-can-surveil-anyone/ ("At its lowest level of investigative activity, on the basis of vague tips or broad intelligence interests, the FBI can follow people with airplanes . . . by opening an assessment, they are allowed to have informants collect information, and they can also physically surveil the subject—including by airplane. . . . According to the DIOG [Domestic Investigations and Operations Guide], some assessments can take whole neighborhoods into their sights, with agents collecting information on the 'composition of the community, the different ethnic groups, religious affiliations, community interests and dynamics, businesses, etc. for analysis and planning.'"). Internal requirements for local and state law enforcement can vary and are often undisclosed.

33. *See* DL Cade, *ARGUS-IS: A 1.8 Gigapixel Drone Camera That Sees Everything and Then Some*, PETAPIXEL (Jan. 28, 2013), http://petapixel.com/2013/01/28/argus-is-a-1-8-gigapixel-drone-camera-that-sees-everything-and-then-some/.

34. Reel, *supra* note 4.

35. *Id.*

II. UNIQUE FEATURES AND PRIVACY RISKS OF AERIAL SURVEILLANCE

Aerial surveillance and its ever-expanding capabilities possess unique features that pose significant privacy risks. It is critical to examine these features, and the applications they provide, in determining to what degree the Fourth Amendment ought to limit aerial surveillance.

A. *Unique Features and Privacy Risks of Aerial Surveillance*

Aerial surveillance possesses a number of unique features that create distinct risks to privacy as compared to other forms of government surveillance. First, aerial surveillance occurs from a vantage point that can view private property on a much larger scale than any form of traditional ground-level surveillance, more easily overcoming civilians' deliberate efforts to conceal private property.[36] Second, aerial surveillance is mobile, presenting the ability to follow moving targets and easily redirect efforts to different targets in a way that stationary cameras, such as police "Blue Light" cameras and traffic cameras cannot.[37] This enhanced mobility is augmented by the openness of airspace, giving aerial surveillance a higher degree of mobility than ground-level officers and vehicles, which are restrained by obstructions. Third, aerial surveillance is inconspicuous. Whereas individuals can regularly notice and develop comprehensive mapping of Blue Light cameras[38] or even beat cops,[39] aerial surveillance is a true panopticon, able to observe anywhere at any time without any notice or warning to those being monitored.[40] Fourth, aerial surveillance can target a wide field, providing the ability to expand access and retain capabilities for precision with minimal capabilities. While the ability to immediately monitor any point in a city requires an

36. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 216 (1986) (involving officers that secured a private plane, flew over defendant's house, and identified marijuana growing in the yard that was shielded from a view at ground level).

37. *See* Geoff Manaugh, *How Aerial Surveillance Has Changed Policing—and Crime—in Los Angeles*, N.Y. TIMES MAG. (Mar. 23, 2016), https://www.nytimes.com/2016/03/27/magazine/panopticops.html?_r=0.

38. Jennifer Helsby, *Police Surveillance in Chicago*, LUCY PARSONS LABS, https://redshiftzero.github.io/policesurveillance/#cameras (last updated Jan. 19, 2016).

39. *See* Sam Sanders, *Officers Ask Map App to Remove Police Tracking*, NPR (Jan. 28, 2015), http://www.npr.org/sections/thetwo-way/2015/01/28/382013185/officers-ask-map-app-to-remove-police-tracking.

40. *See* Reel, *supra* note 4.

enormous allocation of manpower and technology, aerial surveillance encompasses an incredibly wide field of view with the capability to rapidly hone in on any area within it at a moment's notice.[41] This is a feature that Persistent Surveillance highlights as a selling point for its services, advertising on its websites that its systems "can show you everything that has happened and track the suspect(s) where they go."[42]

Figure 3: A Persistent Surveillance demo image highlights the system's ability to track a suspect's movements throughout a city. "Here, a suspect is tracked to and from the three locations he robbed."[43]

The ability of aerial surveillance to take advantage of a wide field will become exponentially more powerful as law enforcement moves towards photo resolution technology like the ARGUS-IS, where a camera attached to an aircraft need not sacrifice field of view for precision.

41. *See PSS Law Enforcement Services*, PERSISTENT SURVEILLANCE SYS., http://www.pss1.com/law-enforcement-support (last visited Feb. 17, 2017).

42. *Id.*

43. *Id.*

While law enforcement has argued that pervasive aerial surveillance is nothing more than an indistinct expansion of police CCTV programs,[44] these unique factors show that it is fundamentally different and give police significantly more power.

B. *Location Identification and Tracking*

One especially troubling manner—both in terms of privacy protections and Fourth Amendment rights—in which these unique features give police new power is in the field of location identification and tracking.

In recent years, location tracking has become a common investigative police tactic.[45] Typically, this occurs via tracking cell phones either through cell-site location data, phones' GPS information, or a combination of both. Aerial surveillance offers law enforcement the means to dramatically expand its location tracking abilities in a number of ways.

First, aerial surveillance can identify a target's location—either through a zoom in or in conjunction with ground-level surveillance—then zoom out to a wider level and simply track the small, previously identified target for an extended period of time.[46] This is in fact what the Baltimore Police Department and Persistent Surveillance boast as a feature employed as part of their aerial surveillance programs.[47]

Aerial surveillance location tracking can also be aided by "tagging technologies," i.e., technologies that can identify individuals in an automated manner based on certain traits.[48] Two particular tagging technologies, license plate readers[49] and facial recognition

44. Kevin Rector, *Baltimore's Aerial Surveillance Program Goes Way Beyond Citiwatch, Experts Say*, BALT. SUN (Aug. 25, 2016), http://www.baltimoresun.com/news/maryland/crime/ bs-md-ci-surveillance-differences-20160825-story.html.

45. For example, Verizon received 135,786 requests for cell phone location data in the first half of 2016. *See* VERIZON, TRANSPARENCY REPORT 1H (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-1H-2016.pdf.

46. Reel, *supra* note 4.

47. *Id.*

48. Jake Laperruque & Joe Onek, *How a Chain Link Fence Can Protect Privacy in the Age of "Collect It All*," LAWFARE (May 9, 2016), https://www.lawfareblog.com/how-chain-link-fence-can-protect-privacy-age-collect-it-all.

49. CATHERINE CRUMP, AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 2 (July 2013).

technology,[50] have seen rapid development in capabilities and increased use by law enforcement in recent years.[51] These technologies will make location tracking via aerial surveillance easier by reducing manpower needed to track individuals. With sufficient resolution, an automated system could track the path of a person or car without any human effort. More disturbing, tagging technologies could allow aerial surveillance to surreptitiously focus on a specific site and monitor its attendees. This action poses serious danger to privacy and Fourth Amendment rights.[52]

Tagging technologies are not the only video analytics tool that will enhance the power of aerial surveillance. There are a variety of other tracking technologies that could augment aerial surveillance effectiveness, though at a lower resolution, and also increase the government's ability to engage in unprecedented forms of surveillance. For example, the tracking technology, BriefCam, allows law enforcement to overlay hours of video and then isolate individuals based on certain factors so monitors can view all applicable targets with hours of time reduced to minutes.[53] This can be used to isolate all individuals or cars that are a particular color,[54] or traveling on a specific route.[55] With such technologies, police could "reverse-engineer" location tracking, picking a route they want to monitor, then use BriefCam to immediately isolate and identify everyone who used it over the course of several hours.

With these unique features, and augmented by new technologies, aerial surveillance could permit mass tracking of individuals. This is at odds with evolving legal protections for location privacy and provides the potential for abuse.

---

50. CLARE GARVIE ET AL., GEO. LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP, UNREGULATED POLICE FACE RECOGNITION IN AMERICA 9 (Oct. 18, 2016), https://www.perpetuallineup.org/sites/default/files/2016-10/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law.pdf.

51. *See id*. at 72; *see also* CRUMP, *supra* note 49, at 5.

52. *See infra* Part III.

53. *See Technology,* BRIEFCAM, http://briefcam.com/security/product/ (last visited Feb. 17, 2017); *What We Do*, BRIEFCAM, http://briefcam.com/about-us/#what-we-do (last visited Feb. 17, 2017).

54. *See* BriefCam VS, *BriefCam Video Synopsis*, YOUTUBE (Sept. 1, 2016), https://www.youtube.com/watch?v=86l1RotubDU.

55. *See* BriefCam VS, *BriefCam for Investigations: Who Took A Right At The Intersection?*, YOUTUBE (Dec. 14, 2015), https://www.youtube.com/watch?v=PB2M-e9iq7c ("It takes just under a minute to sort through hundreds of objects and view the relevant ones. Only 9 out of 400 objects took a right at this intersection—review it all in 24 seconds.").

III. POTENTIAL ABUSE OF AERIAL SURVEILLANCE

Aerial surveillance's unique and growing capabilities to identify and track location risks serious potential abuse given first, the current lack of requirements of suspected wrongdoing and independent approval and second, the capability to reveal sensitive location and, in the absence of legal checks, target sensitive activities and vulnerable groups.

A. *Capability to Circumvent Rules and Checks on Location Tracking*

As previously described, location tracking is a common investigative tool, typically conducted by tracking a target's cell phone.[56] However, police obtain such information from companies through court orders that, at a minimum, require reasonable suspicion and, in some states[57] and subject to ongoing litigation,[58] a probable cause warrant. Such measures follow concurring opinions, issued by five Supreme Court Justices in the landmark case *United States v. Jones*, announcing there is a Fourth Amendment privacy right to one's location, even in public.[59]

However, aerial surveillance circumvents these requirements. Beyond general restrictions for flight, there are currently no rules prohibiting use of aircraft for government surveillance.[60] Thus while police would need to at least demonstrate reasonable suspicion—and in many jurisdictions, probable cause—before a court engages in location tracking of a specific suspect, law enforcement can sidestep this requirement by using aerial surveillance. Given developing capabilities, law enforcement may be able to direct

56. *See supra* Part II.B.

57. *See Cell Phone Location Tracking Laws By State*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/map/cell-phone-location-tracking-laws-state (last visited Feb. 17, 2017).

58. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016).

59. *See* United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring).

60. *See generally* GREGORY MCNEAL, BROOKINGS, DRONES AND AERIAL SURVEILLANCE: CONSIDERATIONS FOR LEGISLATORS 2 (Nov. 2014), https://www.brookings.edu/wpcontent/uploads/2016/07/Drones_Aerial_Surveillance_McNeal_FINAL.pdf (describing how most laws regulating surveillance aircrafts focus on how the technology works rather than concerns about privacy); Michael Frank, *Drone Privacy: Is Anyone in Charge?*, CONSUMER REP. (Feb. 10, 2016) (explaining that, although some states have passed laws protecting privacy for the use of drones, broader reaching laws have not been passed, and it is not clear who should regulate such privacy).

such efforts not only to high profile suspects, but also to large numbers of individuals with no connection to illicit activities.

B. *Capability to Reveal Sensitive Information*

Location data can be highly revealing of sensitive personal information and interactions, giving government immense power. The implications of this are clearly stated by Justice Sotomayor in *Jones*:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . . The Government can store such records and efficiently mine them for information years into the future . . . . And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility" . . . . [T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[61]

Justice Sotomayor was speaking in reference to the attachment of a GPS tracking device to a vehicle, but aerial surveillance presents the exact same risks in amplified form. Government ability to store and query location data has only grown since *Jones* was decided in 2012. Aerial surveillance is becoming cheaper, and a single plane or drone can be used to monitor significantly more people than a GPS device.[62] Aerial surveillance is far more surreptitious—there is absolutely no contact, and sometimes the aircraft will be invisible to humans on the ground. In combination with tagging and tracking technologies, limited police resources do not have a diminishing effect on the number of targets that can be tracked. And as the months-long secret nature of the Baltimore spy-plane program demonstrates, aerial surveillance can currently occur with no community notice, and thus no risk of hostility or backlash.

---

61. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).
62. *See* MCNEAL, *supra* note 59.

Unfortunately, despite the Supreme Court ruling unanimously in *Jones* that use of a GPS tracking device required a warrant, due to technologies and techniques like aerial surveillance, the risk of unchecked location tracking that is "inimical to democratic society" has only grown.[63] It is not hard to depict the harms of unrestricted surveillance that bypass the checks established by *Jones* and for cell-site tracking. Again, looking to Justice Sotomayor's concurring opinion:

> Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.[64]

Perhaps most disturbingly, while this type of information gathering was imagined with regard to a tracking device that would log all of an individual's locations—including infrequent stops at sensitive spots—aerial surveillance can also be focused at sensitive locations, logging the identity of everyone who goes there. These sensitive locations could themselves become the target of aerial surveillance, leading to a highly efficient dragnet that can log every single attendee. A police drone or plane could train cameras on a protest, political rally, or mosque and use tagging technology to identify and catalog every single person.

Past and future government action indicate such conduct is a realistic scenario, not just a baseless dystopian fear. We need not look back to the long and troubling examples throughout the twentieth century of politically[65] and racially[66] motivated surveillance to demonstrate this. In recent years, law enforcement agen-

63. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *id.* at 404 (holding 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, constitutes a 'search'").

64. *Id.* at 415 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

65. *See American Big Brother: A Century of Political Surveillance and Repression*, CATO INST., https://www.cato.org/american-big-brother (last visited Feb. 17, 2017) (noting the "federal government's penchant for surveilling" individuals' political activities).

66. *See* Alvaro M. Bedoya, *The Color of Surveillance,* SLATE (Jan. 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html (noting how several civil rights leaders and others, were tracked due to fears of communism).

cies have directed surveillance efforts at Muslim communities[67] and Black Lives Matter protesters.[68]

And while such conduct has received criticism, it shows no signs of abetting. During the 2016 presidential election, President Trump called for surveillance of mosques[69] on numerous occasions,[70] as well as a national database of all Muslims living in the United States.[71] Surveillance of Muslims was recommended to President Trump during the transition period by Congressman and former Homeland Security Committee Chair, Peter King, who explicitly invoked the infamous discontinued New York Police Department ("NYPD") program as a model for nationwide surveillance.[72] Similarly, during his campaign, President Trump accused the Black Lives Matter movement of calling for the murder of police officers and said he would direct the Attorney General to investigate the group.[73] During his confirmation, Attorney General Jeff Sessions refused to rule out using advanced surveillance technologies to target and catalog individuals engaging in protests, religious activities, or political rallies.[74]

With aerial surveillance's current and improving capabilities, this type of surveillance directed at religious minorities and protesters could occur on a mass scale, with a detailed cataloging of

67. *Factsheet: The NYPD Muslim Surveillance Program*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program (last visited Feb. 17, 2017) (discussing the NYPD's surveillance efforts such as spying and mapping, which lead to several negative consequences).

68. George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Protesters Since Ferguson*, INTERCEPT (July 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.

69. Reena Flores, *Donald Trump: "I Want Surveillance of Certain Mosques*," CBS NEWS (Nov. 21, 2015), http://www.cbsnews.com/news/donald-trump-i-want-surveillance-of-certain-mosques/.

70. *See, e.g.*, Jeremy Diamond, *Trump Doubles Down On Calls for Mosque Surveillance*, CNN (June 15, 2016), http://www.cnn.com/2016/06/15/politics/donald-trump-muslims-mosque-surveillance/.

71. Jeremy Diamond, *Trump Would 'Certainly Implement' National Database for U.S. Muslims*, CNN (Nov. 20, 2015), http://www.cnn.com/2015/11/19/politics/donald-trump-barack-obama-threat-to-country/.

72. Christopher Mathias, *Rep. Peter King Urges Donald Trump to Create a Federal Muslim Surveillance Program*, HUFFINGTON POST (Dec. 15, 2016), http://www.huffingtonpost.com/entry/peter-king-muslim-surveillance-trump_us_5852fdcae4b0b3 ddfd8bc377.

73. Reena Flores, *Donald Trump: Black Lives Matter Calls For Killing Police*, CBS NEWS (July 19, 2016), http://www.cbsnews.com/news/donald-trump-black-lives-matter-calls-for-killing-police/.

74. *Nomination of Jeff Sessions to be Attorney General of the United States: Questions for the Record*, 115th Cong. 19–20 (2017) (questions posed by Sen. Richard Blumenthal), https://www.judiciary.senate.gov/imo/media/doc/Sessions%20Responses%20to%20Bluementhal%20QFRs.pdf.

thousands, perhaps even millions of individuals. And under current law it could completely escape any independent checks on accountability.

IV. CURRENT AND PROPOSED LEGAL STANDARD FOR AERIAL SURVEILLANCE

Current case law permits aerial surveillance absent any judicial authorization. The key controlling case is *California v. Ciraolo*, a 1986 case in which the officers in a low-flying plane, roughly 1000 feet altitude, saw marijuana being grown in a backyard and used this observation as the basis to obtain a warrant and conduct a search.[75] The Court ruled that because the marijuana crops were within view of anyone flying in this airspace, there was no reasonable expectation of privacy.[76] The Court solidified this holding in its 1989 decision, *Florida v. Riley*, when under similar circumstances it ruled that an aerial view into a greenhouse from a police helicopter did not violate the Fourth Amendment under *Ciraolo*.[77] Several states have restricted or prohibited the use of drones for law enforcement purposes;[78] however, these restrictions would do nothing to limit an aerial surveillance program similar to the one operated in Baltimore via Persistent Surveillance, or the use of drones for aerial surveillance by federal law enforcement agencies.

Given the deficient ability of current law to check aerial surveillance and prevent broad surveillance of non-illicit activities—including those most fundamental and critical to a democratic society—a new standard to address modern government capabilities and societal needs is appropriate.

The basis for developing a new Fourth Amendment standard in light of new technology and its capacity for enhanced surveillance or, more specifically, a clarified standard with new rules for new technological situations has precedent. It is the basis of the concurring opinions in *Jones*,[79] and is expressed explicitly in the 2014

75. California v. Ciraolo, 476 U.S. 207, 209–10 (1986).

76. *Id*. at 215.

77. Florida v. Riley, 488 U.S. 445, 450 (1989).

78. *See Current Unmanned Aircraft State Landscape*, NAT'L CONF. OF ST. LEGIS. (Jan. 5, 2017), http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

79. *See* United States v. Jones, 565 U.S. 400, 417–19, 430 (2012) (Sotomayor, J., concurring).

Supreme Court opinion, *Riley v. California*, which amended the search exigent to arrest exception to exclude cell phones:

> Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. . . . But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. . . . [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house. . . . 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.[80]

The principle of *Riley* is simple and logical: new technologies that augment the government's surveillance abilities justify changing or, at the very least, expanding existing Fourth Amendment doctrines to apply new circumstances to these technologies.[81]

Such an expansion could be done with the aerial surveillance doctrine of *Ciraolo*. Therefore, the doctrine expressed in *Ciraolo* should be expanded to differentiate between aerial surveillance seen by the naked eye with the surveillance observed via other technologies. This would not only be consistent with *Ciraolo*, but would build upon circumstances highlighted by the Court as key in adjudicating the case.

In *Ciraolo*, the Court emphasized:

> [T]he question remains whether *naked-eye observation* of [the yard] . . . violates an expectation of privacy that is reasonable . . . [however t]he Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe *what is visible to the naked eye*.[82]

Modern aerial surveillance as described in this article is fundamentally different than the type of naked eye aerial surveillance described in *Ciraolo*, just as a police tail is fundamentally different from the GPS tracker in *Jones*, and just as a briefcase is fundamentally different from the cell phone in *Riley*. In all cases, modern technology has created a situation, unforeseeable in light of the original Fourth Amendment doctrine, that unbalances government power and maintenance of privacy in a manner that is necessary for democratic society. And in all cases, features can be added to the doctrine to clarify new rules in application to those technologies.

---

80. Riley v. California, 134 S. Ct. 2473, 2489, 2491, 2495 (2014).
81. *See id*. at 2484–85.
82. California v. Ciraolo, 476 U.S. 207, 213, 215 (1986) (emphasis added).

Here, the "Naked Eye Rule" would build upon *Ciraolo* in the following manner: *aerial surveillance cannot be used by law enforcement absent court approval, unless the surveillance is akin to the naked eye view of a human on the aircraft.* This would have two practical restrictions: first, it would limit unregulated aerial surveillance observations to those obtained at human eye resolution; and second, it would prohibit unregulated use of drones, and any observations that cannot be made by a human on an aircraft.

The practical effect of this rule would be reasonable in terms of legitimate law enforcement and government objectives. First, law enforcement could still engage in low-altitude surveillance, such as with police helicopters, absent court approval. Second, law enforcement could engage in more invasive aerial surveillance, such as tracking a target's movements with a drone or high-altitude aircraft, so long as they demonstrate appropriate cause to a court. Third, the government could engage in aerial surveillance for non-law enforcement purposes absent approval, such as use of drones for wildfire observation.

Finally, the Naked Eye Rule would work in conjunction with the exigent circumstances exception. This could preserve the most critical and noncontroversial uses of aerial surveillance programs, such as the Baltimore program. Under such a system, a city could employ Persistent Surveillance to keep a plane roving in the air, but not recording. Then, in response to an emergency situation—such as an active shooting—the aircraft could immediately begin monitoring and recording the location in question. Such emergency situations could possibly be aided by use of a pre-event video buffer, whereby a very short period of video is continuously recorded and deleted. This could allow aerial surveillance to rapidly respond to exigent circumstances and provide key information—such as the identification of individuals at a location just prior to an active shooting—without the risk to privacy of continuous mass collection and data storage through aerial surveillance. However, implementation of a pre-event video buffer would be controversial and require further evaluation in terms of consistency with Fourth Amendment principles and practical impact.

CONCLUSION: A FIRST STEP FORWARD

The Naked Eye Rule may be viewed as a radical leap, designed to draw a hard line against government use of emerging technologies. However, such a limit has occurred repeatedly before for technologies such as thermal imaging,[83] augmented listening devices,[84] and tracking devices.[85] In contrast, courts' refusals to directly adapt to technological advances have negative and illogical impacts on privacy. For example, modern telephone communications are protected by the Fourth Amendment, yet e-mails are not.[86] In terms of aerial surveillance and the capabilities it provides to law enforcement, we are not only approaching a point of illogic in light of *Jones* and rules for cell-site tracking, but also a serious risk to basic privacy.

The Naked Eye Rule, as proposed here, should not be seen as a leap, but a small step. As articulated in this article, it intentionally leaves open the question of what standard of suspicion must be met before a court. Different forms of aerial surveillance—such as monitoring a specific location, tracking a specific person, or open ended surveillance of a broad area—may be best served by different requirements, as may different degrees of surveillance, such as time for which a person is to be tracked or expanse of area to be monitored. These questions deserve more detailed deliberation before a strict standard is set.

The Naked Eye Rule also leaves open many issues regarding miniaturized drones too small to readily notice, including: What will become the lowest airspace such drones can fly over private property before their conduct becomes trespass? Should restrictions exist on use of such drones to eavesdrop unnoticed on private conversations or read e-mails and text message on a phone "over one's shoulder," so long as the micro-drone is in public?

---

83. Kyllo v. United States, 533 U.S. 27, 40 (2001).

84. *See* Silverman v. United States, 365 U.S. 505, 506–07, 509–12 (1961) (holding that the use of an augmented listening device accompanied by a physical intrusion violated the Fourth Amendment). *But see* Goldman v. United States, 316 U.S. 129, 134–35 (1942), *overruled by* Katz v. United States, 389 U.S. 347, 352 (1967) (holding that the use of an augmented listening device without physical encroachment did not violate the Fourth Amendment).

85. *See* United States v. Karo, 468 U.S. 705, 715–16 (1984); United States v. Jones, 565 U.S. 400, 402 (2012).

86. *See About the Issue*, DIGITAL DUE PROCESS, https://digitaldueprocess.org/about-the-issue/ (last visited Feb. 17, 2017).

Far too often technology outpaces law, with costs to civil liberties in the interim. We are already moving into such a void with regard to aerial surveillance, and it appears the resulting harms to privacy will only continue to grow. The concept of the Naked Eye Rule can act as a step forward towards restoring a balance of law and technology, but there is a formidable amount of discussion, debate, and action that must be undertaken to address the privacy issues examined here. Hopefully, we will work to do so.