Spring 2023

Is Wide-Area Persistent Surveillance by State and Local Governments Constitutional?

Joseph Lake

Is Wide-Area Persistent Surveillance by State and Local Governments Constitutional?

By Joseph Lake

Claremont Graduate University
2023

Approval of the Dissertation Committee

This dissertation has been duly read, reviewed, and critiqued by the Committee listed below, which hereby approves the manuscript of Joseph Lake as fulfilling the scope and quality requirements for meriting the degree of Doctor of Philosophy in Political Science with concentrations in American Politics and Public Law.

Ralph Rossum
Claremont McKenna College
Former Henry Salvatori Professor of American Constitutionalism

Jean Schroedel
Claremont Graduate University
Professor Emerita of Political Science, Former Thornton F. Bradshaw Professor of Public Policy

Melissa Rogers
Claremont Graduate University
Associate Professor of International Studies

Abstract
Is Wide Area Persistent Surveillance by State and Local Governments Constitutional?

by

Joseph Lake

Claremont Graduation University 2023

This dissertation addresses the following question: “Can wide-area persistent surveillance (WAPS) developed by the United States military and employed abroad as a tool in the Global War on Terror be employed domestically as a law enforcement tool without violating the US Constitution’s Fourth Amendment?” The most likely and controversial application of WAPS by state and local governments is for law enforcement. Aircraft will loiter over a city persistently taking high-definition photographs to capture locations of unidentified persons with the intent to identify persons and areas of interest for criminal investigations. Based on the Flyover Cases, aerial surveillance has few constitutional limitations which WAPS can be consistent. The key challenge in determining the constitutionality of WAPS depends on the Court’s interpretation of the Fourth Amendment concerning emerging technologies. Legal scholars have suggested various forms of the Mosaic Theory, which was introduced in two concurring opinions in *Jones v. United States*. The Supreme Court has been reticent to engage new technology’s constitutionality. WAPS is among the less intrusive tools when compared to other emerging technologies like digital information or facial recognition. This research argues why the Courts should view Personal Identifying Information (PII) as the line of reasonable expectations of privacy for WAPS and other emerging technologies. Aerial surveillance by nature, collects passive information, new data is not being created by photographing the happenings in public spaces from an aerial platform. In *Carpenter v. United States*, the Court ruled that warrantless surveillance of cell site location information (CSLI) for more than seven days was an

unreasonable search. However, the court repeatedly referred to CSLI as “unique,” whereas “conventional surveillance and tools, such as security cameras,” are not. WAPS should not be limited by the Constitution for the operational duration, time of day/night, camera resolution, location of collection, altitude, or any other variable at the collection stage of the operations. The analysis and exploitation of WAPS data encounters constitutional limits necessary to protect individuals’ PII absent probable cause standards.

Dedication

Dedicated in memoriam of Dr. Michael Uhlmann

Acknowledgments

Dr. Uhlmann and Dr. Schroedel made up the supermajority of my coursework instruction. Their collegiality, friendship, and respect through important and contentious issues provided invaluable lessons for life in the personal and professional spheres. In this era of divided political values, they provided steadfast care and concern for one another beyond their political disagreements reminding their students how to disagree well. I must also thank them both for seeing potential in me years before I knew it existed in myself. Dr. Schroedel empathized with my self-doubts as a first-generation college graduate. She showed me how my unconventional experiences and skills were assets to research in the field and the lab.

I thank Dr. Scott Waller of Biola University for throwing the first proverbial “rock in my shoe” to consider graduate school. He also saw potential in me that I did not recognize years in advance. He is and has remained a friend and mentor over these years. As a former student of Dr. Uhlmann and Dr. Schroedel he knew two mentors who would invest in and encourage the next generation of political scientists.

I thank Dr. Darren Guerra for the mentorship and friendship he has provided as his student, teaching assistant, and colleague through the years.

Table of Contents

"I've come up with a set of rules that describe our reactions to technologies:
1. Anything that is in the world when you're born is normal and ordinary and is just a natural part of the way the world works.
2. Anything that's invented between when you're fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it.
3. Anything invented after you're thirty-five is against the natural order of things." Douglas Adams, The Salmon of Doubt.

Chapter 1

In August 2016, Bloomberg Businessweek broke the news that the Baltimore Police Department (BPD) had been participating in a pilot surveillance program since the beginning of the year. For months, this platform took high-resolution pictures at a rate of one per second for up to 10 hours a day. The images were of high enough resolution that any person in line-of-sight of the Cessna circling above the city at 8500 feet could be tracked while they remained visible outside. The images were transmitted to an office in Baltimore where an analyst cell waited for specific violent crime reports to be reported to law enforcement. Once a report was received, analysts would zoom in on the location and time of the report to use the images to paint a story of what happened. This program was funded by a private out-of-state grant and fulfilled by Dayton-based Persistent Surveillance Systems (PSS).[1]

Politically complicating the matter, BPD officials deliberately and purposefully hid the program's existence from any elected official in Baltimore's government, against the will of PSS founder and President Ross McNutt, a retired Air Force astronautical engineer who helped develop the military version of this platform more than a decade earlier for use in the Global War on Terror. Due to the secretive nature of the program, the article led to public outcries, and the pilot program concluded. This was not the first time PSS had media attention. Two years earlier, the Washington Post reported on McNutt and PSS's capabilities and operations in Juarez,

[1] Monte Reel, "Secret Cameras Recording Baltimore's Every Move from Above," Bloomberg Businessweek, August 23, 2016, https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ accessed July 21, 2020.

Mexico, Philadelphia, Baltimore, Compton, and Dayton for shorter-term pilot programs to demonstrate their capabilities.[2] The article focused on the 200 hours of surveillance PSS conducted in Dayton for law enforcement purposes at a discounted rate but also mentioned PSS provided imagery of flood in Iowa and Hurricane Sandy aftermath. PSS advertises applications beyond law enforcement, including major event security, emergency response, environmental management, and border security.[3] The distinct form of aerial surveillance conducted by PSS and US military surveillance assets is known as Wide Area Motion Imagery (WAMI).

Statement of the Problem

It is unclear if the use of Wide Area Motion Imagery and the persistent surveillance it may provide by state and local governments is constitutional. I argue any aerial imagery surveillance is constitutional as long as the imagery does not reveal personally identifiable information (PII) without probable cause. Wide Area refers to a specific sensor array of multiple high-resolution cameras stitched together to provide a high-resolution image covering several square miles. The degree of detail and width of the area covered depends on the cameras' resolution and the altitude of the sensors. If the sensors fly at an altitude of 10,000 feet, they will have a smaller scope but more detailed images than if they flew at 20,000 feet. The Motion Imagery references the frequency of the sensor array. It is not a video recorder; the images captured are still. PSS operates the most well-publicized WAMI systems in the United States. Their systems take one image per second and compare that to a standard smartphone video recording that records 30 frames per second. The images stitched together are not entirely

[2] Craig Timberg, "New Surveillance Technology Can Track Everyone in Area for Several Hours at a Time," Washington Post, (Feb. 5, 2014), accessed 28 July 2021, retrieved from 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.
[3] Ross McNutt, "Wide Area Surveillance in Support of Law Enforcement," Persistent Surveillance Systems, January 2014.

smooth; however, they are sufficient to maintain a positive tracking of points of interest, people in view, and vehicles.

The resolution of the camera array is a significant distinguishing feature. A standard high-definition 1080p television's (1920 x 1080) single image is 2.07 megapixels (MP). A 4K digital image (4096 x 2160) is approximately 8.84 MP. The Hawkeye II sensor array fielded by PSS is 192 MP. They boast a coverage area of 64 square kilometers with a discernable resolution at ½ meter.[4] At a practical level, this level of resolution can view people and vehicles. However, any person seen at the zoomed-in resolution cannot be identified in any way. A person appears as a single pixel; age, race, gender, clothing, or limb movements cannot be articulated. These camera systems are only the second generation of the technology family, which is about twenty years old.

Arthur Holland Michel's *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All* details the history, development, and growth of WAMI and supporting technologies. Holland Michel's book provides a definitive history of WAMI from its inspiration on a scientist's date night, the predominately military-backed development of the technology, the fielding of multiple platforms by the United States Government in overseas military operations, and the continued development and attempted domestic deployment of these systems. Michel's book provides a good introduction and background to the creation and operations of wide-area persistent surveillance of the United States military.[5] The legal implications are cursory, as are many of the periodical publications and the few academic publications directly concerning WAMI.

Wide-area surveillance takes the otherwise well-settled doctrine of aerial surveillance and raises tensions because the "soda straw" effect no longer limits the cameras. These provide

[4] Ross McNutt, "Wide Area Surveillance in Support of Law Enforcement," Persistent Surveillance Systems, and January 2014.
[5] Arthur Holland Michel, *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All*, HMH Books, Kindle Edition.

a wide axis of adjustable view and often include high-resolution cameras with long-range and night vision capabilities. The soda straw effect is the loss of surrounding imagery when a camera zooms in on a specific target or area of interest.[6] These camera systems have been used by law enforcement agencies for day and night surveillance since the early 2000s.[7] The cameras have significant zoom capabilities. However, as the lens zooms in, the surrounding area is lost. Wide Area surveillance cameras are high enough resolution that zoom functions are still possible, but the surrounding areas are no longer lost. These wide-area camera arrays were designed and are effective for collecting city-wide images to support the nation-building strategies in the post-Cold War era. The technology has provided "near real-time"[8] for active duty units for over a decade. The collection of images from a single 8-hour flight yields thousands of images capturing a range of activities, legitimate and illegitimate. The forensic application of this data is the particularly challenging point at issue. The persistent use of WAMI over a given area is known as Wide Area Persistent Surveillance (WAPS).

The primary value of WAPS was found in the forensic analysis for investigations following events of interest. During operations in support of the Global War on Terror (GWOT), the first generations of WAMI were unable to positively identify persons of interest. It was able to establish ingress/egress routes and locations perpetrators originated from and exfiltrated. Once locations of interest were identified, analysts could trace the individual's movement from the places of interest to other locations. The information yielded was the development of organized

---

[6] Kim Zetter, "NYPD Helicopter Views Faces from Miles Away," Wired Magazine, last modified June 5, 2008, accessed July 21, 2021, https://www.wired.com/2008/06/nypd-helicopter/

[7] Austen Ian, "For the Spy in the Sky, New Eyes," News, New York Times, last modified June 20, 2000, accessed April 24, 2021, https://www.cds.caltech.edu/~murray/courses/cds101/fa02/caltech/steadycam.html.

[8] "Near real-time" refers to live support but accounts for the seconds or minutes lag between the collection of the platform and the analyst's ability to access the data. For example, during combat operations in Iraq and Afghanistan in support of the Global War on Terror, UAS analysts provided near real-time support to ground forces as they cleared spaces by identifying possible improvised explosive devices and other potential threats in the area from above.; "The New Face of Intelligence," Cayman Compass, 4 July 20210, accessed 29 July 2021, retrieved from https://www.caymancompass.com/2010/07/04/the-new-face-of-intelligence/

network behaviors instead of just apprehending the perpetrators of the event. In the GWOT, improvised explosive devices (IEDs) were the primary threat to the United States and coalition forces. However, those who planted the IEDs were often unimportant actors in the regional battlespace. The network analysis from the forensic data provided information compartmented operation cells would not necessarily share with their members. In a classic form of intelligence analysis, IED cell operations would require human or signals intelligence to identify. Using WAPS abroad made imagery intelligence a key contributor in counter-IED operations.

The primary controversy over WAMI is the potential domestic surveillance applications for law enforcement. The challenge of persistent surveillance and wide-area surveillance can each easily prompt concern. This technology's original military and intelligence applications were not designed to be concealed or diminished. Whenever military-grade technology is applied to potential domestic applications, it is important to be as transparent as possible to encourage public trust and uphold the principles of representative government. The Intelligence, Surveillance, and Reconnaissance (ISR) understanding of “persistent surveillance” refers to the ability to endure multiple hours continuously. According to the United States Joint Forces Command, the formal definition of Persistent Surveillance is “An ISR strategy to achieve surveillance of a priority target that is constant or of sufficient duration and frequency to provide the joint force commander the information to act in a timely manner.”[9] In less strategic language, the purpose of persistent surveillance was to make more actionable intelligence by collecting contextual information instead of sending an unmanned aerial system (UAS or drone) to an improvised explosion location after the fact. Such surveillance was limited at that point to only providing battle damage assessments. Persistent surveillance systems allowed the ability to conduct forensic analysis of the area before the event. For example, suppose an area has had a

[9] “Commander’s Handbook for Persistent Surveillance version 1.0,” United States Joint Forces Command, Joint Warfighting Center Joint Doctrine Support Division, Suffolk, June 2011, accessed 23 April 2021 https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/surveillance_hbk.pdf

concentration of violent crimes in an urban area. Someone reports a crime. The imagery analyst would “rewind” the pictures to target suspicious persons or vehicles in the vicinity of the reported incident. Those persons and vehicles of interest would then be backtracked to identify which buildings they came. This process would rapidly identify locations of interest for further investigation. Obtaining a positive identification would have to be ascertained through additional sources of information via other surveillance systems like facial recognition on the more invasive end of the spectrum or public records of residency on the analog end of the spectrum. As additional events occur, the value of the collection multiplies. WAPS was tested in Dayton, Los Angeles, and for several months in 2016 and 2020 in Baltimore.[10]

The application for law enforcement use relies on the forensic capabilities of WAPS. Unlike the cell structures in the theater of war, the primary persons of interest are those present when a violent crime occurs. WAPS can identify individuals in proximity to events of interest and trace their movements within the coverage area. If the WAPS program lacks ground-level cross-correlating surveillance assets, places of interest can still identify addresses of interest for investigators. When the WAPS system includes additional surveillance assets, persons of interest can be tracked until those ground-level assets capture an image of people in the vicinity of the WAMI, synchronized by the timestamp tracking of the individual. At the operational level, facial recognition, license plate readers, security cameras, social media, cellular site location information, smartphone image metadata, and other emerging technologies can integrate with and enhance WAPS operations.

One of the challenges was the limited number of legal analyses of this emerging technology before 2020. Following a Bloomberg Businessweek exposé of a WAPS pilot

[10] Angel Jennings, Richard Winton, James Rainey, “Sheriff’s Secret Air Surveillance of Compton Sparks Outrage,” Los Angeles Times, April 23, 2014, accessed July 19, 2022, https://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html

program externally funded in Baltimore during the summer of 2016,[11] two law review articles sought to assess the constitutionality of WAPS in 2018.[12] Cumulatively those articles have six citations as of July 2021. In the summer of 2020, with the knowledge and support of elected officials, the Baltimore Police Department started the Aerial Investigation Research Pilot Program (AIR). The program lasted until October 2020. The contract has not been renewed. Mayor Scott has pledged not to reactivate the AIR program during his tenure.[13] The terms and conditions of the AIR program were rigorous, arguably much more strict than necessary, to pass constitutional muster, which the Fourth Circuit panel initially agreed.[14] However, in June of 2021, an 8-7 En Banc panel of the Fourth Circuit reversed and remanded the three-judge panel's decision. Chief Judge Gregory was the dissenting judge on the three-judge panel and wrote the opinion for the En Banc panel.[15] This case did not decisively rule on the constitutionality of law enforcement's use of WAPS. The motion was for the AIR Program's temporary restraining order (TRO). Although the AIR program was discontinued, the imagery data was stored and used for ongoing investigations. The stored data was no longer permitted for use following the En Banc panel's ruling. This case and the accompanying reports will be analyzed more thoroughly in Chapter 7 as a case study. The City of Baltimore did not appeal to the United States Supreme Court. Per the contract of the AIR program, NYU School of Law conducted a constitutional

[11] Monte Reel, "Secret Cameras Recording Baltimore's Every Move from Above," Bloomberg Businessweek, August 23, 2016, https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ accessed July 21, 2020.
[12] John Pavletic, "The Fourth Amendment in the Age of Persistent Aerial Surveillance," 108 J. Crim. L. & Criminology 171 (2018). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4; Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 167-196.
[13]Emily Opilo, "Spy Plane Not Likely to Fly over Baltimore Again, Mayor Says." Baltimore Sun, December 28, 2020. https://www.baltimoresun.com/politics/bs-md-pol-brandon-scott-interview-20201228-ti75hqctsffgrbyggpzdz2xtgm-story.html.
[14] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 979 F.3d 219 (4th Cir. 2020)
[15] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 979 F.3d 219 (4th Cir. 2020)(en banc), https://www.ca4.uscourts.gov/opinions/201495A.P.pdf

assessment of the program, RAND Corporation released a preliminary report on the statistical impact of the AIR program, and the University of Baltimore conducted a community survey.[16]

The primary focus of this analysis is to conduct a rigorous constitutional analysis of WAMI technology and WAPS to identify the existing bright line tests which are sufficient to judge WAPS constitutionality. Much of the constitutional analysis will be focused on the law enforcement use of WAPS. It is in the enforcement of the law that the most robust and controversial jurisprudence has developed for civil liberties. After contacting the Policing Project at NYU, they consider the matter of the constitutionality of WAPS a closed issue. They have not developed the analysis for future cases under different conditions. This analysis will provide the framework for courts to consider. I forecast the challenge against the AIR program to be the first of many nationwide. *Leaders of a Beautiful Struggle v. Baltimore Police Department* introduced the common arguments for and against WAPS, but it is not the end. The Fourth Circuit only ruled on the TRO of the discontinued AIR Program. The Court did not rule on the AIR program in its totality or specifically against WAPS. The AIR program added WAPS to Baltimore's pre-existing surveillance infrastructure, including thousands of ground-level cameras part of the Citiwatch program, automated license plate readers (ALPR), and ShotSpotters, which identify and locate gunfire via near real-time audio analysis. Some of the factors which can change the facts for future courts can be any one or more of the following differences: integrated ground surveillance systems, integrated multi-intelligence sensor payloads, community sentiment towards law enforcement, crimes of interest, flight schedules, funding sources, imagery

[16] Barry Friedman & Max Isaacs, "Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program," The Policing Project at NYU Law (November 2020), Accessed 29 June 2021, Retrieved from https://www.policingproject.org/s/AIR-Program-Audit-Report-vFINAL-reduced.pdf; Ann Cotten et al., "Baltimore Aerial Investigation Research Project Findings from the Early Launch Community Survey," Schaefer Center for Public Policy, June 2020, accessed 29 June 2021, retrieved from https://68i.ab1.myftpupload.com/wp-content/uploads/2020/12/AIRCommunitySurvey-Summary-AllHCHP-FINAL.pdf; Andrew R. Morral, Terry L. Schell, Brandon Crosby, Rosanna Smart, Rose Kerber, and Justin Lee, "Preliminary Findings from the Aerial Investigation Research Pilot Program," Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA1131-1.html.

resolution, altitude, coverage area, flight times, night time collection, data retention, data access policies, all of which can be addressed in different Memorandum of Understandings between the client and WAPS providers. This is far from an exhaustive list, but it demonstrates the numerous factors, mainly at the collection stage of the program. The data exploitation and dissemination stages are also ripe for configured fact patterns which can affect constitutional jurisprudence under the current precedents.

On the one hand, WAPS information-gathering potential is novel. This puts it in a similar category of technological innovations associated with social media, facial recognition, cell site location tracking, and thermal imaging cameras, all of which have been addressed in legislatures and courts in recent decades. On the other hand, the technology itself, aerial surveillance, is not as invasive as the other new technologies previously mentioned. Locations are tracked; however, the tracked subjects remain unidentifiable unless additional analysis and cross-correlating data are used. Individuals are tracked, but they have presented themselves in public spaces where no reasonable expectation of privacy can be asserted. These limitations make WAMI less invasive than facial recognition or cell site location, both of which presuppose a positive identification of the individuals being surveilled. The inability to positively identify anyone without additional analysis is the primary safeguard for the general public and simultaneously maintains the potential to meet probable cause standards for criminal investigations. This technology provides a unique opportunity for legal analysis concerning new technology. Unlike facial recognition or cell site location information (CSLI), the Court established well-established, clear, defined precedents concerning aerial surveillance. The uncertainty comes from a proposed new method of interpreting the Fourth Amendment, the Mosaic Theory, and the frameworks adapted from it.[17] Although Justices Alito and Sotomayor

[17] The Mosaic Theory seeks to analyze the totality of surveillance in a post hoc approach to determine if the data collected becomes unreasonable. This is in contrast to the Sequential Approach, which evaluates the reasonableness of each step of the prospective search to determine the legality of the process.

have provided concurring frameworks for potential future applications, no Supreme Court decision has applied the Mosaic Theory as the decisive approach to Fourth Amendment interpretation.

Finally, regardless of the constitutional considerations of WAPS, practical policy considerations should still be made because WAPS is available to private entities. Unless legislatures make tailor-made policies to regulate WAPS, it will likely be deployed across metropolitan areas in the not-too-distant future. My interest is to consider not just the constitutional challenges of WAPS for law enforcement but for potential private and public users and the city and state levels.

The Supreme Court has demonstrated, in several instances, over the recent decades, an unwillingness to address the growing challenges of the digital era and the Constitution's limits.[18] The issue of privacy and the Constitution is precarious at best. Numerous scholars have offered analyses and suggestions to update the Fourth Amendment and its interaction with modern and future technology.[19] Orin Kerr is one of the few who has advised caution for Courts to lead the change process over legislatures.[20]

---

[18] *Carpenter v. United States*, 585 U.S. 2206 (2018); *United States v. Jones*, 565 US 400 (2012); *Riley v. California* 573 US 373 (2014); *Kyllo v. United States*, 533 U.S. 27 (2001).

[19] Among the most prolific include but are not limited to Orin Kerr, Lawrence Lessig, Christopher Slobogin, Marc Blitz, David Gray, Danielle Citron, Priscilla Smith, Rachel Levinson-Waldman, and many others. *See* Orin Kerr, Note 7, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 802-804 (2004) (Kerr lists fourteen articles published in 2003 alone of authors urging the Courts to modify the Fourth Amendment instead of legislatures.)

[20] Ibid; Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it," 72 George Washington Law Review 1208 (2004), https://ssrn.com/abstract=421860 or http://dx.doi.org/10.2139/ssrn.421860; Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007); Kerr, "Do We Need a New Fourth Amendment?," 107 Michigan Law Review 951 (2009); Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011); Orin Kerr, "Why Courts Should Not Quantify Probable Cause" (March 28, 2011). *The Political Heart of Criminal Procedure: Essays on Themes of William J. Stuntz* (Michael Klarman, David Skeel, and Carol Steiker, eds), pages 131-43 (Cambridge 2012), https://ssrn.com/abstract=1797824; Orin Kerr, "The Mosaic Theory of the Fourth Amendment" (April 1, 2012), 111 Michigan Law Review 311 (2012), https://ssrn.com/abstract=2032821; Orin Kerr, "The Effect of Legislation on Fourth Amendment Protection (August 8, 2016), 115 Michigan Law Review 1117 (2017), https://ssrn.com/abstract=2819878; *United States v. Carpenter* Brief amicus curiae of Professor Orin Kerr, 2 Oct 2017, SCOTUSblog, https://www.scotusblog.com/wp-content/uploads/2017/10/16-402-bsac-Orin-Kerr.pdf; Orin Kerr,

The Supreme Court of the United States (SCOTUS) has taken over two hundred cases concerning the Fourth Amendment's "unreasonable searches and seizures." In a 2013 60 Minutes interview with Justice Sotomayor discussing constitutional interpretation philosophies, Justice Sotomayor explained, "what does unreasonable mean? What's a search and seizure? On those three words, search, seizure, and unreasonable law books are filled. Shelves and shelves of them are filled."[21] From those hundreds of cases that have contributed to the present interpretation of the Fourth Amendment, no fewer than twenty cases are essential to analyze the Fourth Amendment concerns of WAPS. An additional forty-eight cases via precedents upon precedents have created numerous competing tests, interests, and narrow foci.[22] Because "privacy" does not explicitly appear anywhere in the Constitution, the concept of it in the federal legal realm has had to identify it piecemeal until there was sufficient support that the legal bodies could identify such an abstract concept. I have categorized the 200+ cases into five categories: property (39%), criminal (69%), intimacy (9%), First Amendment (8%), and regulatory/special needs (17%).[23] Many cases fall into multiple categories, which is common in civil rights litigation. For example, during the Civil Rights Era, many cases where the Court granted teeth to the Equal Protection Clause of the Fourteenth Amendment also cited the Due Process Clause. Likewise, as the Equal Protection Clause expanded further than matters of racial equality, gender equality jurisprudence was also based on the Equal Protection Clause and Due Process Clause. The Fourteenth Amendment is easily the source of most civil rights litigation, including the Fourth Amendment, via the Due Process guarantees of the Fourteenth.

The five categories of Fourth Amendment cases demonstrate the complexity of the right to privacy. There are volumes of scholarly works critical of the formation of the right to privacy,

---

"Implementing Carpenter" (December 14, 2018), *The Digital Fourth Amendment* (Oxford University Press), Forthcoming, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257

[21] Sonia Sotomayor, "Constitution: A living document or not?" Interview by Scott Pelley, January 13, 2013, Video, 2:31, https://www.youtube.com/watch?v=kHvgiEWH6A4

[22] See Table 1 (Excel Table of Key Fourth Amendment Cases for WAPS)

[23] See Appendix A (Excel Formation of the Right to Privacy)

particularly after *Katz*'s "reasonable expectation of privacy" criteria was established. Because these categories have such a broad range, Fourth Amendment scholars have often divided their focus into these more niche categories. Compared to First Amendment scholars who are likely to focus on Free Speech or Religious Liberty, the parsing of Fourth Amendment scholarship is not due to textual clauses in the amendment but the path of common law, which has developed over the last century. It is mainly due to the blurring of precedents that have developed over the decades. For example, *Griswold v. Connecticut* was the first case to recognize "zones of privacy," to which a married couple's right to access contraceptives was categorized under "intimacy." As the understanding of privacy concerning bodily autonomy continued to develop from *Griswold*,[24] the privacy right concerning the property and criminal cases split from those initial "zones" to the more expansive "reasonable expectation of privacy" in *Katz*.[25] One cannot isolate the right of privacy found in Fourth Amendment jurisprudence apart from *Griswold*; simultaneously, *Griswold* was built upon parental rights, freedom of association, and Due Process.[26]

The first American academic publication which asserted a right to privacy derived its claim from property rights in 1890.[27] Although Professors Warren and Brandeis (later Justice Brandeis) did not cite James Madison's essay on Property, their argument strongly aligned with Madison's generous concept of property rights. For example, Madison's understanding of property included "a property very dear to him in the safety and liberty of his person. He has an equal property in the free use of his faculties and free choice of the objects on which to employ

[24] *Eisenstadt v. Baird*, 405 U.S. 438 (1972); *Roe v. Wade*, 410 U.S. 113 (1973); *Carey v. Population Services International*, 431 U.S. 678 (1977); *Planned Parenthood of Southeastern PA. v. Casey*, 505 U.S. 833 (1992)
[25] *Griswold v. Connecticut*, 381 U.S. 479, 350 (1965)
[26] *Meyer v. Nebraska*, 262 U.S. 390 (1923); *Adler v. Board of Educ. of City of New York*, 342 U.S. 485 (1952); *National Association for the Advancement of Colored People v. Alabama*, 357 U.S. 449 (1958); *NAACP v. Button*, 371 U.S. 415 (1963)
[27] Samuel Warren and Louis Brandeis, "The Right of Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890): 193.

them."[28] Warren and Brandeis' concept of privacy was more narrowly applied to those whose reputations could result in a loss of value, celebrities, and what we would today call paparazzi.[29] Prior to 1890, only two Supreme Court cases implicated the Fourth Amendment. *Ex Parte Jackson* recognized the contents of mail in the federal system to be protected from searches and seizures. However, the exterior markings were not protected.[30] *Boyd v. United States* described "a search and seizure [was] equivalent [to] a compulsory production of a man's private papers," the decision included a much-cited excerpt from *Entick v. Carrington,* a 1765 case identifying the intangible portion of harm caused from violated property and person.[31]

WAPS engages the Fourth Amendment's understanding of property, criminal, and special needs law. There are presently eight different Fourth Amendment doctrines that might apply to WAPS: "reasonable expectation of privacy," Open Fields, Third Party, Plain View, technology "in general public use," "public navigable airspace," "public vantage points," "programmatic searches," and potentially the Mosaic Theory.[32] These doctrines are in question because WAPS is a new technology that enhances aerial surveillance capacities over public and private property. However, it does not physically trespass on private property, and privacy claims cannot be asserted in public space or private property viewable from public space. Finally, if the aerial surveillance is deemed "unreasonable," the degree of harm caused is likely to be permissible against programmatic, special needs searches. These unique characteristics of WAPS are the key reasons why, among the recent new technologies, WAPS is the least

[28] James Madison, "Property," *The Papers of James Madison*. Edited by William T. Hutchinson et al. Chicago and London: University of Chicago Press, 1962--77 (vols. 1--10); Charlottesville: University Press of Virginia, 1977--(vols. 11--).
[29] Samuel Warren and Louis Brandeis, "The Right of Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890): 205.
[30] *Ex parte Jackson*, 96 U.S. 727 (1878)
[31] *Boyd v. United States*, 116 U.S. 616 (1886)
[32] See Table 1: Key Fourth Amendment Cases for WAPS; *Katz v. United States*, 389 U.S. 347 (1967); *Hester v. United States*, 265 U.S. 57 (1924); *Smith v. Maryland*, 442 U.S. 735 (1979); *Coolidge v. New Hampshire*, 403 U.S. 443 (1971); *Kyllo v. United States*, 533 U.S. 27 (2001); *California v. Ciraolo*, 476 U.S. 207 (1986); *Florida v. Riley*, 488 U.S. 445 (1989); *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990); *United States v. Jones*, 565 U.S. 400 (2012)

intrusive when compared to global positioning satellite (GPS) or cellular site location information (CSLI), Automated License Plate Readers, facial recognition software, or geofencing. The Fourth Amendment's text most plainly addresses the protection of property against unreasonable searches and seizures. The difficulty is identifying what is or is not "reasonable" across the decades and centuries of constitutional law.

Table 1: Key Fourth Amendment Cases for WAPS

Case Name	Year	Property	Criminal	Special Needs	Summary	Privacy Protected?	Ruling
Hester v. United States	1924	X	X		Hester dropped a bottle of moonshine while fleeing from Revenue Officers. The officers did not have a warrant and were on the private property of Hester's father. The bottle was abandoned, found in Hester's open fields. The abandoned bottle was not unreasonably searched nor seized.	No	9-0
Carroll v. United States	1925	X	X		Established the "Automobile Exception" that when an arrest is made from an automobile, if the officer has reasonable suspicion of evidence or contraband, a warrant is not required for a search.	No	7-2
Katz v. United States	**1967**		**X**		Law enforcement made an elaborate setup on a set of public phone booths in which a microphone was placed to capture the conversation without intruding on the private space within the booths. Katz sues a motion to suppress because he had a reasonable expectation of privacy. Court agrees to overrule Olmstead.	**Yes**	**7-1**
Camara v. Municipal Court	1967	X		X	Overruled Frank, required building inspectors to gain a warrant outside of emergency conditions. "Primarily applied to administrative searches of residences.	Yes	6-3
United States v. Miller	1976		X	X	ATF subpoenas Miller's bank records to expose an unregulated distillery business. Court holds that Miller's bank records had no right to privacy of his bank records as they were the bank's business records.	No	7-2
Rakas v. Illinois	1978	X	X		Suspects of a robbery during a traffic stop. During the stop, the officer finds an short-barreled rifle and ammunition. The suspects were arrested then claim the search was illegal. Because they did not own either the vehicle or the weapons they had no standing. Defendants must demonstrate a "legitimate" expectation of privacy to make a 4th Amendment challenge.	No	5-4

Smith v. Maryland	1979		X		A Robbery suspect harassed his victim via phone. Police identified his vehicle and owner through registration, then requested a pen register that collected phone numbers. The Court held Fourth Amendment protections only apply to unreasonable government action. This reasonable expectation of privacy does not apply to the numbers recorded by a pen register because those numbers are used in the regular conduct of the phone company's business, a fact of which individuals are aware.	No	5-3
United States v. Knotts	1983		X		Police placed a short-range tracking device in a chloroform container. Using the device to track the vehicle after losing sight, Court ruled a search did not occur.	No	9-0
Oliver v. United States	1984	X	X		Two consolidated cases wherein marijuana was grown in open fields which had signs marking them as private property. The Court applied open fields doctrine to properties with such signs on the basis of the open field over the sign.	No	6-3
Dow Chemical Company v. United States	1986	X		X	Dow denied EPA follow-up on-site inspection, EPA did an aerial inspection of facilities, Court ruled in favor of EPA.	No	5-4
California v. Ciraolo	1986		X		Warrantless aerial surveillance of a backyard does not constitute a search. Ciraolo was growing marijuana in his backyard which was lined with a fence. The aerial naked eye search was sufficient for a search warrant on the property.	No	5-4
Florida v. Riley	1989		X		Florida case of warrantless search over a person’s property with a helicopter. Marijuana was growing in a greenhouse on rural property. Via helicopter and missing roof panels officers were able to identify the marijuana.	No	5-4
Michigan Department of State Police v. Sitz	1990		X		DUI checkpoints found to be consistent with the 4th Amendment, "no one can seriously dispute the magnitude of the drunken driving problem or the States" interest in eradicating it."	No	6-3
Kyllo v. United States	2001		X		Police use a thermal imaging device to scan residence, based on hot spots, utility bills, and informant police acquire a search warrant. Court held the use of the thermal imaging device to be a search. Because the device was “not in general public use” the information gained was a search, otherwise unattainable without entering the residence.	Yes	5-4
Jones v. United States	2012		X		GPS trackers attached to vehicles absent a search warrant are unconstitutional. Court ruled narrowly that the physical placement of the GPS	Yes	9-0

					device on the vehicle constituted a trespass. Majority opinion punted on the issue of warrantless GPS tracking absent physical device. Overturned United States v. Pineda Moreno (2010) 9th Circuit.		
Riley v. California	2014		X		Riley conducts a drive by in San Diego. Several weeks later on expired tags, his car is impounded and he is arrested after two handguns were found in the vehicle. Upon his arrest his phone was seized and searched which revealed gang affiliations that lead officers to connect him to the shooting. The search of the phone was not related to officer safety and the Court agreed the search of his phone to be unreasonable.	Yes	9-0
Carpenter v. US	2017		X		Cell site location information (CSLI) data points are not covered by the Third Party Doctrine after the FBI used the Stored Communications Act to gather locational data points to convict Carpenter of robbing electronics stores. His locational data was co-located with robberies that occurred via CSLI. The Court applied Third Party Doctrine to business records which CSLI were not extended. The Court also found the special nature of CSLI data compared to conventional business records.	Yes	5-4

To properly analyze WAPS technology, one must have a technical understanding of the sensors and assets at issue, an operational understanding of how it is most effectively used, and a legal understanding of the controlling principles which may or may not bless further development. In a recent interview Ross McNutt, one of the creators of WAPS systems and the President of Persistent Surveillance Systems, said there was significant interest in WAPS being adopted in European and Southeast Asian countries.[33] McNutt and PSS made WAPS commercially available for domestic use available in 2007.[34] It is not unreasonable, in my view, to forecast that every major city will consider operating WAPS in the next decade. It is, therefore, necessary to provide a sound legal analysis of the competing interests and a healthy

[33] Doc Bites, Eye in the Sky - Inside America's 24-Hours Airspace Surveillance System, Youtube Video, 10:07, 23 Sept 2020, https://www.youtube.com/watch?v=_ip7JZyaH-E (McNutt declined to disclose which nations specifically were in contact with PSS)
[34] McNutt, Ross, Wide Area Surveillance in Support of Law Enforcement, Persistent Surveillance Systems, January 2014.

dose of pragmatism about the Digital Age to form acceptable guidelines that might inform the public of the costs and benefits. Only when the people being directly affected are informed can the potential for good policy exist in a representative system of government. I believe the Fourth Amendment is implicated when individuals are implicated. Therefore, when stage agents collect personal identifying information (PII), probable cause must be established if not a warrant is granted for such a search to commence.

Legislators, likewise, have been slow to address the concerns posed by these new technologies. Local governments have been more proactive, particularly concerning facial recognition[35] and unmanned aerial surveillance systems.[36] However, technologies continue to develop faster than legislators can skillfully deliberate about the costs and benefits each new kind of technology can offer.

Theoretical Framework/Methodology

In this research, I will use legal research to analyze the constitutional doctrines and policy questions about fielding WAPS over the major cities in the United States by state and local governments. I will also apply these analytical methods to analyze Baltimore's Aerial Investigative Research (AIR) Pilot Program. A three-judge panel in the Fourth Circuit Court of Appeals addressed a temporary restraining order on the AIR program in *Leaders of a Beautiful Struggle v. Baltimore Police Department* in November 2020. The fifteen-judge en banc panel

[35] Fight For the Future, Ban Facial Recognition Map, banfacialrecognition.com accessed July 21 2021, https://www.banfacialrecognition.com/map/ (This map includes state, county, and local jurisdictions which have banned facial recognition technology for law enforcement use.)
[36] Jonathan Bates, "Current Unmanned Aircraft State Law Landscape," National Conference of State Legislatures, last modified 20 Jan 2021, accessed July 21 2021 https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx#:~:text=Nine%20states%E2%80%94California%2C%20Kentucky%2C,for%20utilities%2C%20defense%20and%20railroads.

ruled in June 2021, reversing the three-judge panel decision.[37] The present controversy over this technology is primarily surrounding law enforcement deployment of these sensors; as Michel introduces, Ross McNutt of PSS argues, and I will elaborate, there are numerous applications this technology can aid. The scope of this paper will not address the national security implications or potential scenarios which could induce national security claims to instigate more complex constitutional considerations which would likely impact state and local implementation of WAPS. Historically speaking and depending on the state of affairs, the Courts have given broad powers to address national security emergencies with significant degrees of deference to the executive bodies under its War Powers authority. Therefore, the constitutional analysis of WAPS will address only state and local bodies implementing this surveillance technology for their respective jurisdictions and interests. Depending on how federal courts analyze WAPS for cities and states to implement, it would not be unexpected that federal bodies might provide subsidies for various reasons, including interagency cooperation, data analysis, or national security interests. The scope of publications specifically addressing WAPS is very limited in political science and legal publications. Publications directly addressing WAPS are mostly in the computer science and engineering fields discussing how to make WAPS more technologically efficient and reliable. Numerous graduate-level publications from Army and Air Force colleges address persistent surveillance technologies, primarily from the interest and

[37] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 979 F.3d 219 (4th Cir. 2020)(en banc), https://www.ca4.uscourts.gov/opinions/201495A.P.pdf; further references to this case will be *LBS v. Baltimore*.

perspective of national security.[38] The United States military has used WAPS technology since 2006.[39]

Thesis

Wide Area Persistent Surveillance (WAPS) takes the previously non-intrusive technology of aerial surveillance and combines it with big data capacity to challenge the sufficiency of the Fourth Amendment. WAPS operated by State or local governments may or may not be Constitutional. Current precedent can aptly be made for either argument depending on the conditions of WAPS use and which Fourth Amendment doctrines are applied. If the sequential approach to the Fourth Amendment is applied, as long as WAPS does not identify individuals or persist for more than six continuous consecutive days, it is likely constitutional. If the Mosaic Theory or its derivatives are applied, WAPS could not be constitutionally permissible. Regardless of constitutionality, domestic WAPS is coming to major cities across the nation in the near future, either by government entities or private parties. Therefore, legal and political

---

[38] Daniel Schmitt, "Automated Knowledge Generation with Persistent Video Surveillance" Masters' Thesis, (Air University, 2006), accessed 25 June, 2020, retrieved from Air Force Institute of Technology, https://scholar.afit.edu/cgi/viewcontent.cgi?article=3560&context=etd; Todd Hogan, "The Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority?," Masters Thesis, (U.S. Army Command and General Staff College, 2007), accessed 25 June 2020, retrieved from Homeland Security Digital Library https://www.hsdl.org/?view&did=232599; Cristina Fekkes, "Defining Conditions for the Use of Persistent Surveillance" Master's Thesis, (Navy Postgraduate School, 2009), accessed 25 June 2020, Retrieved from Dudley Knox Library https://calhoun.nps.edu/handle/10945/4444; U.S. Joint Forces Command, "Commander's Handbook for Persistent Surveillance," Joint Warfighting Center (Joint Doctrine Support Division 2011), accessed 23 April 2021, retrieved from Joint Chiefs of Staff https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/surveillance_hbk.pdf; Daniel Gouré, "Wide Area Persistent Surveillance Revolutionizes Tactical ISR," Lexington Institute, 28 November, 2012 accessed 23 June, 2020, https://www.lexingtoninstitute.org/wide-area-persistent-surveillance-revolutionizes-tactical-isr/; James A. Ratches, Richard Chait, and John W. Lyons, *DTP-100: Some Recent Sensor-Related Army Critical Technology Events*, National Defense University Press (2013) accessed 23 June 2020, https://ndupress.ndu.edu/Portals/68/Documents/DefenseTechnologyPapers/DTP-100.pdf?ver=2017-06-22-143033-827; Hesham Aly, "How the Military Can Integrate Unmanned Aerial Systems in the Civil Reserve Air Fleet," Master's Thesis,. (Air University, 2016). Retrieved from Defense Technical Information Center accessed 19 May, 2019. https://apps.dtic.mil/sti/citations/AD1040989

[39] Arthur Holland Michel, *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All*, HMH Books, Kindle Edition.

considerations must be made concerning who operates the platforms, maintains the data, has access to the data, and for how long?

Chapter 2

Background and History

In 1998, on a date night, an unnamed researcher from the Lawrence Livermore Research Laboratory was inspired by watching Tony Scott's blockbuster Enemy of the State.[40] The initial pursuit was to create the kind of imagery satellites depicted in the film. The satellite networks depicted in the film captured large high-resolution tracts of space in a format used not only for near real-time surveillance support of government operations but also forensically to backtrack people and areas of interest. It did not take long before the fiscal barriers put the concept on hold; launching satellites at that time was prohibitively expensive. Additionally, satellites in orbit over the earth move too quickly to maintain surveillance on a given area of interest for periods of time necessary to be considered persistent surveillance; in 2001, the researcher partnered with John Marion, who pursued a similar imagery system at the time in order to track the weather. A failed attempt at funding from the National Reconnaissance Office stymied the initial development due to the $50 million price tag on a working prototype. The prohibitively expensive satellite cost quickly resolved the solution to be atmosphere-bound, and the Livermore Research Lab was able to build a first-generation camera for under $100,000.

By 2003, the insurgency in Iraq was at the top of the headlines, and US forces were encountering improvised explosive devices (IEDs) with deadly effects. The CIA and Pentagon looked to the Jason Defense Advisory Panel, a collection of top scientists across multiple fields who addressed national security challenges, to find the solution to IED attacks. By early 2004, it was clear the solution was not in identifying those who planted the IEDs. The insurgents

[40] Arthur Holland Michel, *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All*, HMH Books, Kindle Edition.

operated by cell structures that built, funded, and placed the devices. The individuals who planted the IEDs were often low-level insurgents, or local residents extorted or threatened into planting IEDs. Further complicating the challenge, the IED cells were not centralized but often operated in independent areas. Hence the surveillance system would need to view the area at large versus focus on particular points of interest. The intelligence community focused on the command, control, and support structure of the IED cells. The intelligence solution was WAPS.

Funded by the money split between the CIA and Pentagon's Rapid Reaction Technology Office, the Lawrence Livermore Research Lab went to work. The imagery was combined with MIT-developed software that stitched the images together, "The resulting imagery had the appearance of a moving satellite image—like Google Earth, but alive."[41] A demonstration of this imagery inspired Steve Suddarth during a counter-IED research mission in the Fall of 2004. Suddarth combined forces with the US Air Force and Los Alamos National Lab, the same that conducted the Manhattan Project. With the help of seed money from the CIA's Intelligence Technology Innovation Center, Suddarth and company developed what would be known as Angel Fire, a four-camera WAMI system that provided real-time surveillance support.[42] Both Constant Hawk and Angel Fire were fielded in manned fixed-wing aircraft.

Due to innovative rivalry between Livermore and Los Alamos, Livermore produced Sonoma, a six-camera, 66-million-pixel WAMI system. Sonoma could monitor a thirty-square-kilometer area, accomplishing what would take thousands of Predator drones' Full Motion Video (FMV) to monitor. The Army Research Laboratory adopted the Sonoma camera, mounted it to a Predator drone, and named it Constant Hawk in 2006. In true competing fashion, the Sonoma camera was packed with one thousand pounds of multi-core computers built by the Lincoln

[41] Arthur Holland Michel, *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All*, HMH Books, Kindle Edition.
[42] Stacia Zachary, "Angel Fire Surveillance a Key Tactical Asset," Eglin Air Force Base News, January 23, 2009, https://www.eglin.af.mil/News/Article-Display/Article/392767/angel-fire-surveillance-a-key-tactical-asset/

Laboratory to stitch the imagery together. Constant Hawk was not able to provide real-time support like Angel Fire was. Instead, couriers would transport the commercial hard drives every few days to Ramstein Air Base in Germany and a National Geospatial-Intelligence Agency facility in Virginia, where the imagery would be analyzed, assessed, and exploited by various intelligence analysts. Deployed in the summer of 2006, Constant Hawk was originally slated to operate for 90 days over Baghdad; it ended up staying until 2011, when most US forces withdrew from Iraq. By 2007, ground forces in Afghanistan requested Constant Hawk, which was fielded in January 2009. In two years, a single Constant Hawk system collected 10,000 hours of surveillance in Afghanistan. Nathan Crawford, who deployed with Constant Hawk and maintained, estimated "600 US service members, and countless Iraqi civilian lives, were spared thanks to operations involving Constant Hawk."[43] At the other end of the spear, Task Force Observe, Detect, Identify, and Neutralize (ODIN) estimated that in the first year of Constant Hawk operations in Iraq, more than 3,000 suspected insurgents were "eliminated" and captured.

Constant Hawk and Angel Fire continued to operate in the Global War on Terror battlespace. Funding and continued development of lighter, higher-resolution sensors were sought. One of the objectives was to combine the resources of both systems and provide real-time support to personnel on the ground. Although the platforms were demonstrating significant success, the overall situation in Iraq continued to degrade, prompting additional emergency funds and action to field new systems to support the military operations. Big Safari, an Air Force skunkworks specializing in rapid deployment of classified projects, such as the Distributed Common Ground Station architecture that makes the US drone operations possible,[44] was tasked with developing the next-generation platform. That platform became Gorgon Stare, a program that, according to Holland Michel, remains a secretive program in which numerous

[43] Arthur Holland Michel, Kindle Edition, Location 623
[44] Air Force Distributed Common Ground System Fact Sheet, United States Air Force, October 13, 2015, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/

interviews were abruptly ended at the mention of the name. Constant Hawk and Angel Fire were operated from fixed-wing manned aircraft.[45] Gorgon Stare is an Unmanned Aircraft System (UAS) using the MQ-9 Reaper airframe.[46] The greater payload of the MQ-9 allows the UAS to be equipped with ISR and multirole payloads and maintain longer flights than their more well-known predecessor, the MQ-1/RQ-1 Predator.[47]

In November 2006, the Defense Advanced Research Agency (DARPA) approved the development of the Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS). With funding from the Rapid Reaction Technology Office of the CIA, 176 5-millimeter cell phone camera chips were arranged to build a camera that could collect 880 million pixels in each frame; this sensor was named Multi-Aperture Sparse Imager Video System (MASIVS). In November 2007, DARPA awarded BAE Systems an $18.5 million contract to build the ARGUS camera. BAE's design would use 368 cell camera chips from the same manufacturer as the iPhone. At the same time, Graphics Processing Units (GPU) used in computers, mainly computer-based gaming, also developed at rates outpacing Moore's Law. These technological boosts in the commercial arena provided the more powerful and lighter hardware that would be used in the next-generation platforms. What was 1,000lbs of multicore computers in the first Constant Hawk was replaceable with BAE's processing unit the size of a couple of shoeboxes with "33,000 processing elements."[48] By August 2009, the ARGUS camera was 1.8 gigapixels which would provide 27.8 gigabytes of raw data each second. During testing, at 10,700 feet,

[45] David Walsh, "EMARSS: The Hawker Beechcraft Turned Spy Plane," Aviation Today, 30 May 2018, accessed 27 July 2021, http://interactive.aviationtoday.com/emarss-the-hawker-beechcraft-turned-spy-plane/; Stacia Zachary, "Angel Fire Surveillance a Key Tactical Asset," Team Eglin Public Affairs (Eglin Air Force Base Press Release), 23 January 2009, accessed 27 July 2021, https://www.eglin.af.mil/News/Article-Display/Article/392767/angel-fire-surveillance-a-key-tactical-asset/

[46] Previously known as Unmanned Aerial Vehicles (UAV)

[47] MQ-9 Reaper Fact Sheet, United States Air Force, 23 Sept 2015 (current as of March 2021), accessed 27 July 2021, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/ ; MQ-1B Predator Fact Sheet, United States Air Force, 23 Sept 2015, accessed 27 July 2021, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/

[48] Arthur Holland Michel, Kindle Edition (Location 541)

heat radiating from the ground and vehicle windshield wipers were visible. The limiting factor at that point was the architecture that could download and store the data.[49] For example, according to Lawrence Livermore National Laboratory, 1.8 gigapixels, at 12 frames per second, create about 600 gigabits per second. That is about 6,000 terabytes (TB) of video data per day.[50]

One would need 180 petabytes (PB) of storage to maintain a month of ARGUS data. According to Forbes, magnetic tape or hard disk drive digital storage for commercial data retention costs between $10-30/TB.[51] For Baltimore's AIR program, the data was stored for three months unless it was being used in an investigation. Three months of ARGUS imagery would amount to 540 million gigabytes of data. If the client were to look to Amazon Web Services (AWS) for data storage, it would cost just under $2,000,000 per month.[52] The cheaper option of magnetic tape physical hard drive storage would still cost $5,000,000 to $15,000,000, not accounting for the additional costs of the physical storage, which would need cooling and maintenance as a data center without the protections of cloud storage. Physical storage could easily make even the lower-cost form factor prohibitively expensive for high-resolution WAPS. Because of these logistical and financial burdens, ARGUS-level imagery for state and local applications is very unlikely. The current cost for PSS to operate over a city is $2,500,000 per year. Additionally, the higher resolution WAPS would be more likely to induce constitutional violations from imagery. ARGUS is detailed enough to read a vehicle license plate from 20,000ft above the area of interest. Such detail would have a resolution that could positively identify individuals, triggering a different, more strict set of Fourth Amendment doctrines. Because

[49] Arthur Holland Michel, Kindle Edition (Location 541)
[50] Sebastian Anthony, "DARPA Shows off 1.8-Gigapixel Surveillance Drone, Can Spot a Terrorist from 20,000 Feet," ExtremeTech, accessed 15 April 2021, https://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet
[51] Tom Coughlin, "Digital Storage Projections For 2020, Part 1," Forbes, December 21, 2019, accessed 24 April 2021 https://www.forbes.com/sites/tomcoughlin/2019/12/21/digital-storage-projections-for-2020-part-1/?sh=5e082f31581c
[52] Amazon Web Services Pricing, accessed July 21 2021, https://aws.amazon.com/s3/pricing/

ARGUS-level resolution would allow positive identification, it would likely cross into the territory of “dragnet-type law enforcement practices,” a more significant constitutional injury than the present issue.[53]

In 2010, Gorgon Stare was deployed at 80% readiness, as Big Safari is known for, and technical problems were frequent. Between the technical difficulties and requests for additional funding, the program was in jeopardy. It survived, and in the Spring of 2011, four MQ-9 Reaper drones were deployed to Afghanistan. They covered more than a 4-kilometer wide area and could transmit to ten ground stations in near real-time. Additional data was sent to Distributed Ground Station (DGS-1) at Langley Air Force Base in Virginia and DGS-2 at Beale Air Force Base in northern California for further Processing, Exploitation, and Dissemination (PED).[54] In 2014 Big Safari delivered 18 units of second-generation Gorgon Stare. This model included day and night cameras, could cover between 40 and 100 square kilometers depending on the altitude, sent out up to 30 chip-out streams to ground units, and had the capacity for additional classified payloads.[55] In 2015, Gorgon Stare was deployed to Syria to support operations against the Islamic State of Iraq and the Levant (ISIL/ISIS). As of 2018, the Department of Defense has been seeking to improve the architecture that would allow operators to be farther than the 500 miles they are currently limited from the platform.

At the same time these platforms were being developed, through Hiper Stare, a National Geospatial-Intelligence Agency (NGA) program, video surveillance archives were digitally made available to intelligence analysts. Gone are the days of suitcases full of hard drives. Since August 2011, Kestrel surveillance balloons equipped with 440-megapixel cameras were

---

[53] *United States v. Knotts*, 460 U.S. 276, 284 (1983)
[54] Air Force Distributed Common Ground System Fact Sheet, United States Air Force, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/; Jeff Kimmons and Graham Gilmer, Maintaining Advantage: Remaking PED for Today’s Intelligence Needs (Maclean: Booz Allen Hamilton, 2019), https://www.defenseone.com/media/ped-thought-piece-presentedby-booz-allen.pdf.
[55] Arthur Holland Michel, Kindle Edition (Location 902)

tethered to the ground and provided bases and combat outposts with persistent wide-area surveillance. These same balloons are used along the US-Mexico border.[56] Estimated for deployment in 2020, it s the Army's Airborne Reconnaissance Low-Multifunction (ARL-M) platform, a fixed-wing all-weather, day and night aerial intelligence surveillance reconnaissance asset.[57] While the different agencies and branches within the DoD continue to build better hardware, the software is also being improved.

Thus far, this has covered the government's development of WAMI systems for overseas applications. During the DC Sniper Attacks in 2002, the Livermore lab scrambled to deploy the platform to assist law enforcement. The perpetrators were apprehended before it could be fielded. In 2015, the defense firm Harris auditioned their CorvusEye 1500, a WAMI system for Urban Shield, an annual large emergency exercise in the San Francisco Bay Area. Logo Technologies and Commuter Air Technologies maintain an aircraft fitted with a 300-megapixel camera at their domestic facilities, ready to deploy anywhere in the nation within 24 hours. MAG Aerospace and Consolidated Resources Imaging, the company that managed Constant Hawk in Iraq, each has WAMI-equipped fixed-wing aircraft ready to deploy nationwide on short notice. L-3, another major defense contractor, offers its SPYDR ISR aircraft with WAMI capabilities. Northrop Grumman offers its 200-megapixel Hawkeye system for domestic applications. Smaller companies such as Special Operations Solutions, Stevens Aviation, Avcon Industries, Valair Aviation, Support Systems Association, Panopses, and Persistent Surveillance Systems (PSS) all offer WAMI support, primarily for law enforcement.[58] PSS has been the most transparent and active company seeking to deploy WAPS.

---

[56] Adi Robertson, "Homeland Security Using Military Wide-Area Camera to Scan Miles of the Us Border at Once," *Verge*, Apr 2, 2012, https://www.theverge.com/2012/4/2/2919677/homeland-security-kestrel-surveillance-camera-us-mexico-border.

[57] Airborne Reconnaissance Low (ARL), United States Army, https://asc.army.mil/web/portfolio-item/airborne-reconnaissance-low-arl-2/ accessed 22 July, 2020.

[58] Arthur Holland Michel, Kindle Edition (Location 1095)

Air Force Colonel Ross McNutt helped develop Angel Fire. Since his retirement in 2007, he has led the path for the domestic use of WAPS. His company, Persistent Surveillance Solutions, has provided law enforcement support in Dayton, Ohio; Baltimore, Maryland; Daytona Beach, Florida; and Juarez, Mexico. In 2017, Buzzfeed journalists utilized an algorithm to analyze flight paths consistent with ISR aircraft. Buzzfeed identified state and local government-registered aircraft in Phoenix, Mesa, Arizona, Orange, and Los Angeles County Sheriffs' departments. Flight paths were also identified under the authorization of the Ohio State Highway Patrol, including one over Cleveland during the 2016 Republican National Convention, Palm Beach County, Florida, and many other locations across the nation doing surveillance along the southern border and near US military bases.[59]

These domestic applications of WAPS systems have presented academic relevance to this developing technology. 1) Does the Fourth Amendment permit state and local agencies to use these systems in the United States? 2) If not, what constitutional doctrines prevent such technology from being operated by state and local agencies? 3) If so, what precedents permit WAPS under the United States Constitution? 4) What are the limiting factors and case law which must be considered to deploy WAPS in the domestic sphere? In June 2021, the 4th Circuit Court of Appeals en banc panel accepted a temporary restraining order (TRO) application against the Baltimore Police Department's (BPD) Aerial Investigative Research (AIR) program, centered around WAPS. PSS was contracted to fly at least 40 hours a week over the city with their 168-megapixel WAPS-equipped aircraft. Following controversy over the 2016 use of WAPS, the contract had numerous limiting factors to the Processing, Exploitation, and Dissemination (PED) process.[60] Despite the limitations, Leaders of a Beautiful Struggle (LBS), a

[59] Peter Aldhous, "We trained a computer to search for hidden spy planes. This is what it found.," *Buzzfeed News*, August 7, 2017, https://www.buzzfeednews.com/article/peteraldhous/hidden-spy-planes.
[60] PED is a standard terminology from within military intelligence architecture to describe the stage of the information. Processing or collection is the raw data stage in which information is collected. Exploitation is the analyst and aggregation phase. Dissemination is the final stage where the intelligence product or report is to be distributed to non-intelligence units for use.; "Insights and Best Practices Intelligence

grass-roots think tank and policy advocacy group with the support of the American Civil Liberties Union (ACLU), filed for a temporary restraining order to prevent the BPD from operating the AIR program.[61] Baltimore Police Department fielded the AIR program from May 2020 to October 2020, when the funding and term concluded. I will present the legal arguments for and against the constitutionality of WAPS systems. The Supreme Court addressed emerging technologies and the Fourth Amendment several times before, but the status of WAPS systems specifically, is unclear. Multiple significant Fourth Amendment doctrines are likely to be considered in evaluating the Constitution and WAPS systems for law enforcement purposes. In addition to the law enforcement support operations WAPS systems can provide, non-law enforcement applications must also be considered. Any organization or institution dealing in the physical space could find a compelling interest in utilizing the data gathered from WAPS to include; major event security, emergency response, environmental management, commercial behavior, construction development, traffic flow, city planning, and countless other applications. What the smartphone did for the individual's ability to be connected to the world, WAPS provides in the physical space.[62]

Chapter 3

Legal Doctrines of Interest

There is no single precedent or technology which potentially interacts with all the established Fourth Amendment doctrines in the way that WAPS is likely to. Many of these intersecting doctrines pivot based on the purpose of the WAPS and the operating institution. It is

---

Operations," Deployable Training Division (DTD) of the Joint Staff J7 (2019) accessed 27 July 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/intell_ops_fp.pdf

[61] "*Leaders of a Beautiful Struggle v. Baltimore Police Department*," American Civil Liberties Union Cases, accessed 18 July 2020, https://www.aclu.org/cases/leaders-beautiful-struggle-v-baltimore-police-department.

[62] McNutt, Ross, Wide Area Surveillance in Support of Law Enforcement, Persistent Surveillance Systems, January 2014.

necessary to provide an overview summary of these doctrines before analyzing the specific case facts, arguments, and opinions used to assess the constitutionality of WAPS between public and private operations. Case law is preeminent in constitutional interpretation for most of the Supreme Justices. Most legal doctrine discussions will focus on Supreme Court cases because they are the "court of last resort." The lower federal courts will be included as the discussion narrows to persistent surveillance and WAPS. Because the focus is on the Fourth Amendment of the Constitution of the United States, state constitutions were not significantly consulted. Scholarship regularly influences how courts apply or use the doctrines, especially those dealing with emerging technologies. However, scholarship has not negated the essential role case law has had in interpreting constitutional principles or text.

To understand the Fourth Amendment, one must begin with the first principles and purpose. The historical context of the Fourth Amendment was in opposition to the Writs of Assistance held by royal officers, which permitted carte blanche search and seizure abilities on the British colonists under the monarch's blessing.[63] The precise language of the Fourth Amendment exemplifies the lack of clarity from the previous regime such 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.

Like much of the criminal and regulatory schema in the United States, much of the developed legal doctrine concerning the Fourth Amendment could be considered "of recent vintage," in the words of Justice Gorsuch.[64] One of the lasting legacies of the Warren Court was its criminal justice reforms. By far, the most relevant doctrine is also among the most contentious, originating in *Katz v. United States* (1967), where the "reasonable expectation of privacy" is established. The Court's first recognition of a right to privacy was framed in the

[63] *Riley v. California*, 573 U.S. 373, 400 (2014)
[64] Uriah02, "Overcriminalization and Regulatory Law," C-SPAN video. March 25 2017. https://www.c-span.org/video/?c4663543/user-clip-overcriminalization-regulatory-law

contraceptive case *Griswold v. Connecticut* (1961). To be fair, the Court in *Griswold* powerfully cited an older, natural rights-based appeal saying,

> The principles laid down in this opinion [by Lord Camden in *Entick v. Carrington* (1765)] affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employes [sic] 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, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment. Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods is within the condemnation of that judgment. In this regard, the Fourth and Fifth Amendments run almost into each other.[65]

Katz's "reasonable expectation of privacy" was contentious for its subjective nature and remains controversial in its subjectivity and circular logic.[66] Regardless, it is the preeminent interpretive method to determine the constitutionality of a search and seizure in Fourth Amendment jurisprudence. To better clarify the conditions, scholars and jurists have turned to Justice Harlan's concurring opinion that the subjectivity test was twofold, not only a "reasonable expectation of privacy" but also "that the expectation is one that society is prepared to recognize as "reasonable."[67] The questions concerning WAPS are, "does the public have a reasonable expectation of privacy of their outside activities?" in the first place, and second, which may be

---

[65] *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1961) footnote

[66] According to Nexis Uni as of 22 July 2021, *Katz v. United States* has been cited 12,960 times between state (7,181) and federal court cases (5,779), it claims an additional 6,587 citations in law reviews. See *Carpenter v. United States*, 585 U. S. 2206, 2244 (2018)(Among the more colorful castigations of *Katz* is Justice Thomas' dissent in *Carpenter* from a collection of Katz's critics, "the *Katz* regime as "an unpredictable jumble," "a mass of contradictions and obscurities," "all over the map," "riddled with inconsistency and incoherence," "a series of inconsistent and bizarre results that [the Court] has left entirely undefended," "unstable," "chameleon-like," "'notoriously unhelpful,'" "a conclusion rather than a starting point for analysis," "distressingly unmanageable," "a dismal failure," "flawed to the core," "unadorned fiat," and "inspired by the kind of logic that produced Rube Goldberg's bizarre contraptions."); *Kyllo v. United States*, 533 U.S. 27, 34 (2001)(The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable. See 1 W. LaFave, Search and Seizure § 2.1(d), pp. 393–394 (3d ed. 1996); Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 S. Ct. Rev. 173, 188)

[67] *Katz v. United States*, 389 U.S. 347, 361 (1967)

more challenging considering the proliferation of social media and smart devices, “is that expectation reasonable”?

In addition to the “reasonable expectation of privacy” of *Katz*, Open Fields, Third Party, Plain View, technology “in general public use,” “public navigable airspace,” “public vantage points,” “programmatic searches,” and potentially the Mosaic Theory are Fourth Amendment doctrines which are necessary to consider to determine the constitutionality of WAPS. At this point, I will introduce these doctrines to make the viability of their concern to the concept and operation of WAPS. The Flyover Cases are the most applicable and analyzed in the literature,[68] a series of three cases concerning the reasonable expectation property owners had over their private property from aerial observation and surveillance. The Court reasoned the property owners did not have a reasonable expectation of privacy for law enforcement and Environmental Protection Agency (EPA) personnel to fly over and use the information gained from the observation of those flights to achieve probable cause, gain warrants, search property, seize illicit property, and obtain convictions based on the information gained from those initial flyovers. In all three cases, the government agents' use of helicopters and low-flying aircraft to observe, take pictures, and use those pictures for probable cause or regulatory enforcement actions were upheld. In *Ciraolo* and *Riley*, the key deliberative points at issue were if the Federal Aviation Administration’s (FAA) minimum aircraft altitude requirements, which were established for safety purposes, were sufficiently applicable to identify airspace over private property as public space. Respectively, one’s private property ends when the FAA’s jurisdiction of airspace begins. Therefore at 1,000ft for fixed-wing aircraft[69] and 400ft for rotary aircraft,[70] because the airspace above the private property can be used as “public navigable airspace,”[71]

[68] *California v. Ciraolo*, 476 U.S. 207 (1986), *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), and *Florida v. Riley*, 488 U.S. 445 (1989)
[69] *California v. Ciraolo*, 476 U.S. 207, 209 (1986)
[70] *Florida v. Riley*, 488 U.S. 445, 451-455 (1989)
[71] *Florida v. Riley*, 488 U.S. 445, 450-453 (1989)

one does not have a reasonable expectation of privacy. In *Ciraolo*, an anonymous call tipped off law enforcement to marijuana growing in the backyard. At the point of interest, there was an interior 10-foot fence inside the backyard, which officers could not see over from the street. Officers then chartered an aircraft to fly over the property to conduct naked-eye observations with a non-zooming 35mm camera. During the flyover, illegal drugs were identified, probable cause was established, and Ciraolo was arrested and convicted. The Court upheld the flyover in a 5-4 decision stating,

> That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.[72]

The articulation of the "public vantage point" has been the key phrase in which optically-based surveillance technologies have been ruled acceptable in public spaces. Building on and respecting *Silverman v. United States*, the primary trigger of the Fourth Amendment is reserved for interior spaces.[73] In *Silverman*, law enforcement officials used a "spike mike" to pierce an air duct and use the ventilation system as an amplifying microphone. Because the device physically penetrated the space, it was an "[74]unreasonable governmental intrusion." The bright line rule between space with a reasonable expectation of privacy and space without one requires a solid, continuous, physical structure.

Riley developed these requirements more clearly. *Riley* was similar to *Ciraolo* but on a rural property with a lower aircraft altitude and an incomplete roof. The property of interest was obstructed from street view surveillance by vegetation. Law enforcement chartered a helicopter to fly over the property to conduct naked-eye surveillance. During the flyover, marijuana was identified in a greenhouse. Ordinarily, the greenhouse would have obstructed the view;

---

[72] *California v. Ciraolo*, 476 U.S. 213 (1986)
[73] *Silverman v. United States*, 365 U.S. 505
[74] *Silverman v. United States*, 365 U.S. 511-512

however, it was missing panels, and the marijuana was clearly identifiable.[75] According to the court, that neglect disqualified the defendants from claiming earnest effort to protect the space from public view, fulfilling the second part of Justice Harlan's *Katz* concurrence.[76]

Dow Chemical is most significant because the Court upheld the use of high-resolution cameras.[77] The surveillance resulted from a non-cooperative regulatory inspection of the premises authorized by the Clean Air Act. The company maintained a robust security layout that prevented ground-level observations and refused to allow the EPA on the property for on-site inspections. Instead of filing for an administrative search warrant, the EPA chartered a commercial aerial photographer with state-of-the-art cameras capable of identifying "wires as small as ½-inch in diameter."[78] This search was conducted from "public navigable airspace" and deemed reasonable under the Fourth Amendment. The commercial-grade aerial camera was "commonly used in mapmaking"[79] and, therefore, permissible for government deployment. It was not until *Kyllo* that the "common use" principle was more established. The Court did not describe the surveillance as a Programmatic Search or use language which would classify it as such, but surrounding precedents would likely describe it as a Programmatic Search if pressed. The opinion focused on the Fourth Amendment claims against Open Fields, curtilage, and the appropriateness of the EPA's enforcement actions. Because WAPS is inherently concerned with high-resolution aerial photography, these are the most applicable cases that will contribute to the Court's eventual determination, whatever it may be.

The Flyover Cases were not crafted *ex nihilo*. They depend upon the Open Fields Doctrine. Open Fields refers to private property, with or without signage, not in the immediate vicinity of a dwelling to gain the full protection of curtilage.[80] Open Fields applies to open private

[75] *Florida v. Riley*, 488 U.S. 445, 449 (1989)
[76] *United States v. Knotts*, 460 U.S. 276, 284 (1983)
[77] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986)
[78] *Dow Chemical Co. v. United States*, 476 U.S. 238 (1986)
[79] *Dow Chemical Co. v. United States*, 476 U.S. 238 (1986)
[80] *Hester v. United States*, 265 U.S. 57, 59 (1924)

property. In relation to the Open Fields is the Plain View exception. Plain View exception was developed in the context of exceptions during a warranted search[81] and seizure[82] in which items with "incriminating character" are "immediately apparent."[83] The application of the Plain View exception in this context is worth considering in light of the reduced scrutiny vehicles have from reasonable searches compared to that of homes and curtilage. Plain View searches, such as a law officer peering into the windows of a vehicle during a traffic stop, have consistently sustained challenges of excluding incriminating evidence.[84] An essential condition to legally invoke the Plain View exception is that the government agent must have a right to be in the private location.[85] Plain View is not necessary or applicable to public spaces. The Court has never seen it necessary to justify conventional physical observation of public spaces. No reasonable law would require law enforcement officers to approach vehicles or conduct patrols with their eyes closed, wherein they may only open their eyes upon probable cause being gained. Both open fields and vehicle searches pertain to private property, which holds some reasonable degree of expected privacy, but neither warrants the level of protection a dwelling has. In numerous cases, law enforcement officers made legal stops for other issues. However, incriminating evidence from subsequent searches added additional legal enforcement actions to the original traffic violation.[86] The incriminating evidence observed in the plain view of the officer led to the search, seizure, arrest, and conviction of subjects. The WAPS application concerns persistent imagery collection over private and public areas. The primary areas of WAPS interest

[81] *Arizona v. Hicks*, 480 U.S. 321 (1987)
[82] *Coolidge v. New Hampshire*, 403 U.S. 443 (1971)
[83] *Horton v. California*, 496 U.S. 128, 133-137 (1990)
[84] *Carroll v. United States*, 267 U. S. 132 (1925); *Cooper v. California*, 386 U. S. 58, 59 (1967); *Cardwell v. Lewis*, 417 U.S. 583, 589 (1974); *California v. Carney*, 471 U.S. 386 (1985)
[85] *Horton v. California*, 496 U.S. 128 (1990)
[86] *Cooper v. California*, 386 U. S. 58, 59 (1967); *Harris v. United States*, 390 U.S. 234 (1968); *Colorado v. Bannister*, 449 U.S. 1 (1980); *New York v. Belton*, 453 U.S. 454 (1981); *Texas v. Brown*, 460 U.S. 730 (1983); *New York v. Class*, 475 U.S. 106 (1986)

for law enforcement purposes are public spaces. WAPS cannot look into any structures in ways more facially invasive than the facts from *California v. Ciraolo* or *Florida v. Riley*.

Programmatic Search doctrine finds its origin in *New Jersey v. TLO*,[87] in which school administrators physically searched a student's belongings without exigent circumstances or probable cause sufficient for a warrant. The search yielded drug paraphernalia. The Court upheld the search. Justice Blackmun's concurrence explained the reasoning, "Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers."[88] Programmatic Searches have been the basis of several types of searches to include: "stop and frisk,"[89] building inspections,[90] border checkpoints on public highways,[91] mandatory drug tests for drug enforcement agents to qualify for a promotion,[92] DUI checkpoints,[93] mandatory drug test for public school extracurricular activities,[94] and searches of parolees.[95] On balance, Programmatic Searches such as roving border patrols for undocumented individuals,[96] consentless blood draws,[97] and lifetime tracking by a satellite-based GPS bracelet are not protected actions.[98]

"Probable Cause" is the standard law enforcement personnel must meet prior to making an arrest, conducting a search, or receiving a warrant.[99] This requirement is explicitly described

---

[87] *New Jersey v. T.L.O.*, 469 U.S. 325 (1985)
[88] *New Jersey v. T.L.O.*, 469 U.S. 351 (1985)
[89] *Terry v. Ohio*, 392 U.S. 1 (1968)
[90] *Camara v. Municipal Court*, 387 U. S. 523, 537 (1967)
[91] *United States v. Martinez-Fuerte*, 428 U. S. 543, 557 (1976)
[92] *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989)
[93] *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990)
[94] *Board of Education of Independent School District No. 92 of Pottawatomie City v. Earls*, 536 U.S. 822 (2002)
[95] *United States v. Knights*, 534 U.S. 112 (2001) with probable cause; *Samson v. California*, 547 U.S. 855 (2006) without probable cause.
[96] *United States v. Brignoni-Ponce*, 422 U.S. 878 (1975)
[97] *Mitchell v. Wisconsin*, 588 U.S. ___ (2019)
[98] *Grady v. North Carolina*, 575 U.S. ___ (2015)(Per Curiam)
[99] Probable Cause Definition, Legal Law Institute, Cornell Law School, https://www.law.cornell.edu/wex/probable_cause, accessed July 24, 2020.

in the Fourth Amendment. It is the base requirement necessary to justify the state examining a specific member of the public with greater scrutiny than the public at large. Probable cause is distinguished from reasonable suspicion by objective circumstances and evidence. For example, with the AIR program, those standards would be met by a positive detection from the Shotspotter or confirmation from officers responding to a 911 call. There are exceptions when crimes are witnessed in the presence of officers or exigent circumstances require immediate action;[100] such processes can be temporarily delayed. Because of the warrant requirement and necessity of probable cause, WAPS may potentially be a prima facie violation of the Fourth Amendment if it is deemed an unreasonable search according to precedent. This exact argument was one of the arguments of the plaintiffs in *LBS v. Baltimore*.[101]

Kyllo v. United States is a controlling case concerning the use of new technology for surveillance and the Fourth Amendment. The Court established the "general public use" test, which applies to situations where law enforcement uses technology not generally accessible to the public. In 1991, a Department of Interior agent viewed sections of a triplex with a thermal imaging camera from the street. The thermal image indicated excess heat signatures venting from the residence. The agent determined from the thermal readings were sufficient for probable cause that interior marijuana growing was taking place. The agent acquired a warrant using the evidence of the thermal imagery. The residence was searched, and a marijuana grow was identified and seized. The majority opposed the use of thermal imaging technology from the street on the grounds that it identified information that could have otherwise only been acquired from entering the premises. Relying on *Silverman*, the majority reaffirmed the sanctity of activities from within a residence. In *Silverman*, the Court struck down the warrantless use of

[100] *Kentucky v. King*, 563 U. S. 452, 460, 470 (2011); *Brigham City v. Stuart*, 547 U. S. 398, 403–404 (2006); *Caniglia v. Strom*, 593 U. S. ____ (2021); *Lange v. California*, 594 U. S. ____ (2021)
[101] "*LBS v. Baltimore"* will be the used short form of *Leaders of a Beautiful Struggle v. Baltimore Police Department* through the rest of this writing.

"spike mikes"[102] because the spike was an "unauthorized physical encroachment within a constitutionally protected area."[103] The dissent emphasized that the thermal image did not display images through walls but only showed heat venting from the exterior, which "did not invade any constitutionally protected interest in privacy."[104] The majority believed the information revealed by the thermal imager would have otherwise been only acquired through surveillance of the interior of the structure.

The majority applied the General Public Use test, which prohibits law enforcement from using technology otherwise available to the public without a warrant.[105] The majority did not clarify what or when "general public use" is met with new or emerging technologies. Depending on the degree of availability necessary to determine the "general public use,"[106] this may also be a prima facie barrier to WAPS. General Public Use is unlikely to be claimed because PSS has provided services to public and private entities with identical sensor arrays per the client's needs. Whether "general public use" refers to available in general, affordability, accessibility, or another factor is not clear. On the other hand, the photographic chips used in the first generation of ARGUS-IS were from the iPhone 8, technology which is very widely proliferated in general public use. Thus an argument could be made that the high definition capabilities of the

---

[102] *Silverman v. United States*, 365 U.S. 505, 506(1961) ("The instrument in question was a microphone with a spike about a foot long attached to it, together with an amplifier, a power pack, and earphones. The officers inserted the spike under a baseboard in a second-floor room of the vacant house and into a crevice extending several inches into the party wall, until the spike hit something solid "that acted as a very good sounding board.")

[103] *Silverman v. United States*, 365 U.S. 505, 510 (1961)

[104] *Kyllo v. United States*, 533 U.S. 27, 41 (2001)

[105] *Kyllo v. United States*, 533 U.S. 27, 34 (2001), ("To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman*, 365 U. S., at 512, constitutes a search— at least where (as here) the technology in question is not in general public use.")

[106] The General Public Use test for the Fourth Amendment should be distinguished from the Common Use test for the Second Amendment, established in *United States v. Miller*, 307 U.S. 174 (1939) and *District of Columbia v. Heller*, 554 U.S. 570 (2008). The Common Use test for the Second Amendment is used to determine which firearms are constitutionally protected for lawful use. How a court is to determine what "common" is has been established in *Kolbe v. Hogan*, Jr., No. 14-1945 (4th Cir. 2017) and cited by seven federal courts of appeal as of July 2021.

ARGUS-IS sensors would not be the disqualifying factor, so long as it did not cross a different sequential line in the chain of doctrines Fourth Amendment doctrines. Hence, the lower resolution of PSS's Hawkeye I or II cameras is not likely to conflict with the Fourth Amendment on strictly technical comparisons.

The Third Party Doctrine developed after *Katz*'s reasonable expectation of privacy was issued via *Smith v. Maryland*[107] and *Miller v. United States*.[108] In *Smith*, the Court rejected the claim that an individual's phone number being recorded on a pen register, a standard tool telephone companies use to record dialed phone numbers, violated their reasonable expectation of privacy. The majority believed a reasonable person would know telephone companies kept records of the numbers called; this much should have been known based on phone bills.[109] Miller unsuccessfully sought to suppress bank records that revealed evidence of unregulated whiskey manufacturing, possession, and sales. The material at issue was not the records of Miller but the bank's records of Miller's accounts; hence the claim that such records were "private papers"[110] could not apply to documents neither owned nor possessed by Miller. The synergy of *Smith* and *Miller* has borne the Third Party doctrine in which information voluntarily given to third parties, in these cases, a bank and phone company, did not have a reasonable expectation of privacy. This doctrine is potentially the most important when a private agent operates WAPS. One may reasonably conclude that if or when private entities operate WAPS for proprietary purposes, state officers may subpoena those images to investigate criminal reports.

Third Party Doctrine does not end with *Smith* and *Miller*. A more recent and essential case concerning Third Party doctrine and the limits of the reasonableness of Fourth Amendment

[107] *Smith v. Maryland*, 442 U.S. 735 (1979)
[108] *United States v. Miller*, 425 U.S. 435 (1976)
[109] *Smith v. Maryland*, 442 U.S. 735, 742 (1979)
[110] *United States v. Miller*, 425 U.S. 435, 440 (1976)

searches is found in *United States v. Carpenter*.[111] In *Carpenter*, the Court addressed whether the government's access to historical cell-site location information (CSLI), location information from a cellular phone held by the phone carrier to maintain service, was considered a search. One should be reasonably aware that a phone carrier must know the location of a cellular device to maintain connectivity between the mobile phone and the cellular tower signals. Following Smith and Miller's footsteps, such information clearly had no reasonable expectation of privacy. However, under the second part of Justice Harlan's *Katz* concurrence, "the expectation be one that society is prepared to recognize as "reasonable,"[112] Chief Justice Roberts identified a "unique nature of cell phone location records"[113] which overrides "the fact that a third party holds the information."[114] The *Carpenter* majority declined to extend Third Party doctrine to CSLI records if those records track a phone's location for more than seven days by classifying the CSLI data as being in a "qualitatively different category."[115] It should be emphasized that the ruling does not prevent CSLI records from being accessed by government agents. It only raised the bar from a court order under the Stored Communications Act[116] to a warrant requirement for the phone company to provide such records. *Carpenter* was also a long-awaited response to Fourth Amendment jurisprudence and new technology. In the previous decade, the Court only ruled on two cases affecting the Fourth Amendment and new technology. *Riley v. California* requires a warrant for law enforcement to search the data on the

[111] *Carpenter v. United States*, 585 U. S. 2206, 2220 (2018)
[112] *Katz v. United States*, 389 U.S. 361 (1967)
[113] *Carpenter v. United States*, 585 U. S. 2206, 2220 (2018)
[114] *Carpenter v. United States*, 585 U. S. 2206, 2220 (2018)
[115] *Carpenter v. United States*, 585 U. S. 2206, 2220 (2018); Carpenter v. United States, 585 U. S. 2206, 2217 Footnote 3 (2018)
[116] 18 U.S. Code Chapter 121 (2018), (The 2018 amendment was part of the CLOUD Act in a Consolidated Appropriations Act. The CLOUD Act was a legislative response to moot *United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018). The Microsoft Corporation asserted an American citizen's stored data outside the United States did not fall under the Stored Communications Act, the CLOUD Act clarified the physical location of the data storage does not matter for US companies in possession of data on US persons.)

cellular phone of an arrested individual.[117] *United States v. Jones* ruled that government agents may not place a GPS tracking device on a vehicle without a warrant.[118]

In *Jones*, a multi-agency task force investigated illicit narcotics moving between the District of Columbia and Maryland. The task force followed proper procedural requirements and obtained a search warrant which permitted them to place a GPS tracking device on Jones' vehicle. The warrant only permitted collection for ten days. The task force collected and compiled information from the tracking device for 28 days. The location tracking data on Jones was used to convict him at the United States District Court of drug trafficking and conspiracy. The District Court did suppress the location data from when Jones was at his residence but permitted the data when he was in public spaces, including roads. At the D.C. Court of Appeals, Jones challenged the admissibility of the location data, which contributed to his conviction in federal court. The D.C. Circuit Court reversed Jones' conviction "because it was obtained with evidence procured in violation of the Fourth Amendment."[119] The United States appealed to the Supreme Court. The Court granted certiorari. The issue before the Supreme Court appeared to be that of the D.C. Circuit. Was it a search to warrantlessly place a GPS tracking device for a criminal investigation? This was of key importance in the Oral Arguments, including one exchange where Chief Justice Roberts inquired if the members of the Court could be tracked with a GPS device. Deputy Solicitor General Dreeben nervously affirmed the Chief's question.[120] Regardless of the pressing interest in warrantless GPS tracking data and the Fourth Amendment, a five Justice majority sidestepped the question. The majority held that placing the GPS device was a trespass.[121] The majority declined to answer the question about the GPS

[117] *Riley v. California*, 573 U.S. 373 (2014)
[118] *United States v. Jones*, 565 U.S. 400 (2012)
[119] *United States v. Maynard*, 615 F.3d 544, 568, 392 U.S. App. D.C. 291, 315, 2010 U.S. App. LEXIS 16417, *58 (D.C. Cir. August 6, 2010)
[120] Transcript of Oral Argument at 9-10, *United States v. Jones*, 565 U.S. 400 (2012)
[121] *United States v. Jones*, 565 U.S. 400, 404-412 (2012)

tracking data, saying this "leads us needlessly into additional thorny problems."[122] Justice Sotomayor signed with the majority and wrote a concurrence. Justice Alito wrote a concurrence joined by the remaining Justices. Each concurrence introduced its own approach to the Mosaic Theory of the Fourth Amendment, separate and distinct from each other and Judge Ginsburg's criteria in *Maynard*.[123]

Interested parties hoped *Jones* would update the decades-old *United States v. Knotts*[124] and *United States v. Karo*,[125] two cases involving radio transmitting beepers, but the majority declined.[126] In Knotts, police followed a barrel of stolen chloroform with a radio-transmitting beeper for three days. The beeper was placed in the barrel before the theft, following a tip from Hawkins Chemical Company's owners. In *Karo*, a confidential informant sold a drum of ether with a beeper in the barrel and tracked it intermittently for 222 days. In both cases, the Court upheld the use of the beeper in public spaces and open fields, but not when the beeper was moved inside a private residence.[127]

The Mosaic Theory is the most novel and complex doctrine to transform Fourth Amendment jurisprudence if adopted. It is among the most contentious points of debate in present-day discussions on new technology and government surveillance. In this section, only the jurisprudence of Mosaic Theory will be addressed. The literature review in the following chapter will give a deeper analysis. The common concept across the different forms of Mosaic theories is that when otherwise reasonable, exposed details about a person are aggregated into

---

[122] United States v. Jones, 565 U.S. 400, 412, 132 S. Ct. 945, 954, 181 L. Ed. 2d 911, 923, 2012 U.S. LEXIS 1063, *21, 80 U.S.L.W. 4125, 23 Fla. L. Weekly Fed. S 102, 2012 WL 171117 (U.S. January 23, 2012)

[123] *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010)

[124] *United States v. Knotts*, 460 U.S. 276 (1983)

[125] *United States v. Karo*, 468 U.S. 705 (1984)

[126] *United States v. Jones*, 565 U.S. 400, 409, 132 S. Ct. 945, 952, 181 L. Ed. 2d 911, 921, 2012 U.S. LEXIS 1063, *16, 80 U.S.L.W. 4125, 23 Fla. L. Weekly Fed. S 102, 2012 WL 171117 (U.S. January 23, 2012) (Knotts would be relevant, perhaps, if the Government were making the argument that what would otherwise be an unconstitutional search is not such where it produces only public information. The Government does not make that argument, and we know of no case that would support it.)

[127] *United States v. Karo*, 468 U.S. 705, 714 (1984)

a mosaic, intimate, unreasonable details are revealed. As *Katz* proclaimed, all Mosaic theories emphasize that the "Fourth Amendment protects people, not places."[128] Using mosaics is a long-practiced technique within the national security apparatus going back to *CIA v. Sims*.[129] The term "mosaic" was jurisprudentially introduced in *In re United States*,

> It requires little reflection to understand that the business of foreign intelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair. Thousands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate.[130]

There are three distinct definitions to which the Mosaic Theory has been applied. In *Maynard*, Judge Ginsburg's litmus test to meet Justice Harlan's "expectation be one that society is prepared to recognize"[131] was manifest via *Bond v. United States*[132] by what was reasonably "exposed to the public."[133] Maynard exposed himself to the public by driving in public; however, no member of the public would have had access to the totality of Maynard's movement for a month. Therefore, "we hold the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[134] In *Jones*, Justice Alito's concurrence

---

[128] *Katz v. United States*, 389 U.S. 347, 351 (1967)
[129] *CIA v. Sims*, 471 U.S. 159, 161, 105 S. Ct. 1881, 1883, 85 L. Ed. 2d 173, 178, 1985 U.S. LEXIS 2741, *1, 53 U.S.L.W. 4453, 11 Media L. Rep. 2017 (U.S. April 16, 1985) ("Thus, what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.")
[130] *In re United States*, 872 F.2d 472, 475, 1989 U.S. App. LEXIS 4984, *8, 277 U.S. App. D.C. 37, 27 Fed. R. Evid. Serv. (Callaghan) 1003 (D.C. Cir. April 14, 1989)
[131] *Katz v. United States*, 389 U.S. 347, 361 (1967)
[132] Bond v. United States, 529 U.S. 334 (2000)(In Bond, the Court ruled against a US Border Patrol Agent squeezing a "brick-like" object in Bond's canvas bag. The Court held, Bond had exposed his canvas bag to the public, but the squeezing of the bag was not something the public was willing to recognize as a reasonable act.)
[133] United States v. Maynard, 615 F.3d 544, 548, 392 U.S. App. D.C. 291, 295, 2010 U.S. App. LEXIS 16417, *1 (D.C. Cir. August 6, 2010)
[134] United States v. Maynard, 615 F.3d 544, 548, 392 U.S. App. D.C. 291, 295, 2010 U.S. App. LEXIS 16417, *1 (D.C. Cir. August 6, 2010).

primarily criticized the majority for not addressing the pertinent question about the GPS tracking. Justice Alito's criticisms were based on practicality, "if long term monitoring can be accomplished without committing a technical trespass...the Court's theory would provide no protection."[135] His concurrence upheld *Knotts* to deny any reasonable expectations of privacy "in his movement from one place to another " and limited the expectation of privacy against visual observation, even on private property.[136] Nevertheless, he questioned the duration of the collection by adding a "relatively short-term" limitation on the duration of the monitoring.[137] The majority challenged such a time-based concern, "That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated."[138] The Mosaic Theory implicitly adopted by Justice Alito's concurrence thus depended upon what a reasonable person would expect law enforcement to do, a close standard to *Maynard* but sufficiently distinct. Justice Sotomayor criticized the majority for its avoidance of the prompting question, "In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[139] Sotomayor's concern strikes back to Harlan's second condition for the digital age, "whether people reasonably expect that their movements will be recorded and aggregated"[140] in such a way that intimate details of life

---

[135] United States v. Jones, 565 U.S. 400, 425, 132 S. Ct. 945, 961, 181 L. Ed. 2d 911, 931, 2012 U.S. LEXIS 1063, *42, 80 U.S.L.W. 4125, 23 Fla. L. Weekly Fed. S 102, 2012 WL 171117 (U.S. January 23, 2012)

[136] United States v. Jones, 565 U.S. 400, 430 (2012)

[137] United States v. Jones, 565 U.S. 400, 430 (2012), ("Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.")

[138] United States v. Jones, 565 U.S. 400, 412 (2012)

[139] United States v. Jones, 565 U.S. 400, 415, 132 S. Ct. 945, 955, 181 L. Ed. 2d 911, 924, 2012 U.S. LEXIS 1063, *26, 80 U.S.L.W. 4125, 23 Fla. L. Weekly Fed. S 102, 2012 WL 171117 (U.S. January 23, 2012)

[140] *United States v. Jones*, 565 U.S. 400, 416, 132 S. Ct. 945, 956, 181 L. Ed. 2d 911, 925, 2012 U.S. LEXIS 1063, *28, 80 U.S.L.W. 4125, 23 Fla. L. Weekly Fed. S 102, 2012 WL 171117 (U.S. January 23, 2012) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that

might be revealed. She goes on to question the maintenance of the Third Party doctrine.[141] Therefore, depending on what the reasonable expectation of privacy is, what the reasonable person would expect law enforcement to do, what a reasonable person thinks they have exposed to the public, or what a reasonable person expects can be gained from recorded and aggregated data. Each is a subcategory of a Mosaic Theory.

Carpenter v. United States declined to explicitly adopt any one of the criteria of the three kinds of Mosaic Theory. The only appearance of "mosaic" anywhere in the opinion was Justice Thomas' dissent, which cited a Supreme Court Review article, "Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory." The citation was not for its merits but to include it among over a dozen articles deriding the "*Katz* regime."[142] There are passages one could interpret as an openness toward a form of a Mosaic Theory. However, for the court to adopt such a novel shift in Fourth Amendment jurisprudence, it would be less challenging to rely on a new set of "emanations and penumbras."[143] The majority sought to find the balance between *Knotts* and *Smith* and *Miller*.[144] In the summary of *Knotts*, the five justices' concurrence recognized their agreement that the trespass could have been accomplished through digital means, not just physical.[145] The majority acknowledged Justice Alito and Sotomayor's concern over "longer term" monitoring, regardless if the Court accepted *Maynard*'s Mosaic, "whether those movements were disclosed to the public at large."[146] In the next paragraph, the jurisprudential pendulum swung toward *Smith*'s standard, "a person has no legitimate

---

enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.")

[141] *United States v. Jones*, 565 U.S. 400, 417 (2018)("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.")

[142] *Carpenter v. United States*, 585 U. S. 2206, 2244 (2018)

[143] *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965)

[144] *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979); *United States v. Miller*, 425 U.S. 435, 442 (1976)

[145] *Carpenter v. United States*, 585 U. S. 2206, 2214 (2018) ("surreptitiously activating a stolen vehicle detection system" in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone.")

[146] *Carpenter v. United States, 585 U. S. 2206, 2214 (2018)*

expectation of privacy in information he voluntarily turns over to third parties."[147] The balance exercised by the majority declined to extend *Smith* and *Miller* and adopted the time-sensitive portion of *Knotts*.[148] It declined to go further with the *Jones*' concurrences presented by the "qualitatively different category," CSLI data, to provide for the "unique nature" reasoning against explicit adoption of a Mosaic Theory.[149] The majority did leave sufficient phrases where some may interpret an adoption of a Mosaic Theory: "the Government could, in combination with other information, deduce a detailed log of Carpenter's movements,"[150] "time stamped data provides an intimate window into a person's life,"[151] and "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle… individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time."[152] However, without identifying which of the three Mosaics the Court may endorse, implementing one, a combination of the three, or a different approach altogether.[153] The outcome is less likely to be a workable rule than the court sought to update. If the Court were to embrace a paradigm-changing rule to the Fourth Amendment jurisprudence, like a Mosaic Theory, it would not do so in vague terms.

If the Court were to adopt any of the mosaic theories, none of them would sufficiently answer essential questions about its implementation without precise prescriptions to applicable agencies to a degree the Courts tend to avoid. For example, what kind of probable cause hurdles must be met by a human WAPS analyst observing criminal behavior? How many pixels are necessary for an imagery analyst to testify accurately? The closest case that might apply to these questions was *Jones*, where the unanimous Court avoided those classes of questions

[147] *Carpenter v. United States*, 585 U. S. 2206, 2215 (2018)
[148] *Carpenter v. United States*, 585 U. S. 2206, 2217 (2018)
[149] *Carpenter v. United States*, 585 U. S. 2206, 2217 (2018)
[150] *Carpenter v. United States*, 585 U. S. 2206, 2220 (2018)
[151] *Carpenter v. United States*, 585 U.S. 2206, 2218 (2018)
[152] *Carpenter v. United States*, 585 U.S. 2206, 2219 (2018)
[153] Gray, David C. and Citron, Danielle Keats, "The Right to Quantitative Privacy" (March 5, 2013). Minnesota Law Review, Vol. 98, 2013, U of Maryland Legal Studies Research Paper, 2013-23, https://ssrn.com/abstract=2228919

altogether. Instead, the majority opinion avoided the primary policy question by narrowly tailoring the focus on the act of placing the GPS device and not the challenges presented by the new technology. There is no doubt that Justice Scalia's jurisprudence would have led him to emphasize the legislature's role in defining such terms. Justices Alito and Sotomayor, in separate concurring opinions, signaled to readers the concern about developing technology and the lack of congressional guidance. Justice Sotomayor's concurrence also argued for applying the Mosaic Theory, albeit not in such technical terminology. As of the 2022-2023 term, the Court has not provided additional guidance since *Carpenter*. In the 2021-2022 term, the Court denied cert to *US v. Tuggle*, a case concerning persistent surveillance from a pole camera.[154] As technology continues to develop, questions governing the human side of surveillance might be moot before the Courts can articulate the Fourth Amendment in the twenty-first century.

Literature Review

The available legal and political science literature specifically addressing WAMI or WAPS is limited. Much of this section will provide an overview and assessment of the applications and interpretations of Fourth Amendment jurisprudence concerning emerging technologies from the last twenty years. Prior to the developments of Big Data, long-endurance surveillance aircraft, and high-resolution, low-cost photography, such concerns were limited to science fiction. WAMI is widely published in the science, technology, engineering, and math fields. Those articles and studies focus on the technical side of the discussion, such as "how to make it work," not the legal or policy side of the issue.[155] Within the national security context,

[154] *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021)

[155] Rahul Thakkar, "A Primer for Dissemination Services for Wide Area Motion Imagery," *Open Geospatial Consortium*, 2012, accessed 20 June 2020, https://portal.ogc.org/files/?artifact_id=50485; M. D. Pritt and K. J. LaTourette, "Georegistration of Multiple-Camera Wide Area Motion Imagery," *2012 IEEE International Geoscience and Remote Sensing Symposium*, 2012, pp. 1765-1768, accessed 20 June, 2020, https://ieeexplore.ieee.org/document/6351174 doi: 10.1109/IGARSS.2012.6351174.; E. Blasch, G. Seetharaman, K. Palaniappan, H. Ling and G. Chen, "Wide-Area Motion Imagery (WAMI) Exploitation Tools for Enhanced Situation Awareness," *2012 IEEE Applied Imagery Pattern Recognition Workshop*

discussions of WAPS usage are also well-published, however, the use of WAPS in the national security context is mostly outside the jurisdiction of the Fourth Amendment.[156] The historical overview of WAPS addresses this point at length.

WAPS in domestic applications was not widely publicized until 2016 when Bloomberg Businessweek published a 4,000-word profile on PSS and McNutt after a 6-month trial program

(AIPR), 2012, pp. 1-8, accessed 20 June, 2020, https://ieeexplore.ieee.org/document/6528198 doi: 10.1109/AIPR.2012.6528198.; V. Santhaseelan and V. K. Asari, "Tracking in Wide Area Motion Imagery Using Phase Vector Fields," *2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 823-830, accessed 20 June 2020, https://ieeexplore.ieee.org/document/6595967 doi: 10.1109/CVPRW.2013.123.; R. C. Philip, S. Ram, X. Gao and J. J. Rodríguez, "A Comparison of Tracking Algorithm Performance for Objects in Wide Area Imagery," *2014 Southwest Symposium on Image Analysis and Interpretation*, 2014, pp. 109-112, accessed 20 June, 2020, https://ieeexplore.ieee.org/document/6806041 doi: 10.1109/SSIAI.2014.6806041.; J. Prokaj and G. Medioni, "Persistent Tracking for Wide Area Aerial Surveillance," *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1186-1193, accessed 20 June 2020, https://ieeexplore.ieee.org/abstract/document/6909551, doi: 10.1109/CVPR.2014.155.; Vijayan Asari, ed. *Wide Area Surveillance: Real-Time Motion Detection Systems. Augmented Vision and Reality*, Volume 6. Heidelberg: Springer, 2014. https://doi.org/10.1007/978-3-642-37841-6.R.; Hartung Spraul and T. Schuchert, "Persistent Multiple Hypothesis Tracking for Wide Area Motion Imagery," *2017 IEEE International Conference on Image Processing (ICIP)*, 2017, pp. 1142-1142, accessed 20 June 2020, https://ieeexplore.ieee.org/abstract/document/8296460 doi: 10.1109/ICIP.2017.8296460.; N. M. Al-Shakarji, F. Bunyak, G. Seetharaman and K. Palaniappan, "Robust Multi-object Tracking for Wide Area Motion Imagery," *2018 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, 2018, pp. 1-5, accessed 20 June, 2020, https://ieeexplore.ieee.org/document/8707377 doi: 10.1109/AIPR.2018.8707377

[156] Daniel Schmitt, “Automated Knowledge Generation with Persistent Video Surveillance” Masters’ Thesis, (Air University, 2006), accessed 25 June, 2020, retrieved from Air Force Institute of Technology, https://scholar.afit.edu/cgi/viewcontent.cgi?article=3560&context=etd; Todd Hogan, “The Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority?,” Masters Thesis, (U.S. Army Command and General Staff College, 2007), accessed 25 June 2020, retrieved from Homeland Security Digital Library https://www.hsdl.org/?view&did=232599; Cristina Fekkes, “Defining Conditions for the Use of Persistent Surveillance” Master’s Thesis, (Navy Postgraduate School, 2009), accessed 25 June 2020, Retrieved from Dudley Knox Library https://calhoun.nps.edu/handle/10945/4444; U.S. Joint Forces Command, “Commander’s Handbook for Persistent Surveillance,” Joint Warfighting Center (Joint Doctrine Support Division 2011), accessed 23 April 2021, retrieved from Joint Chiefs of Staff https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/surveillance_hbk.pdf; Daniel Gouré, “Wide Area Persistent Surveillance Revolutionizes Tactical ISR,” Lexington Institute, 28 November, 2012 accessed 23 June, 2020, https://www.lexingtoninstitute.org/wide-area-persistent-surveillance-revolutionizes-tactical-isr/; James A. Ratches, Richard Chait, and John W. Lyons, *DTP-100: Some Recent Sensor-Related Army Critical Technology Events*, National Defense University Press (2013) accessed 23 June 2020, https://ndupress.ndu.edu/Portals/68/Documents/DefenseTechnologyPapers/DTP-100.pdf?ver=2017-06-22-143033-827; Hesham Aly, “How the Military Can Integrate Unmanned Aerial Systems in the Civil Reserve Air Fleet,” Master’s Thesis,. (Air University, 2016). Retrieved from Defense Technical Information Center accessed 19 May, 2019. https://apps.dtic.mil/sti/citations/AD1040989

in 2016.[157] PSS and McNutt were also featured in a National Public Radio-sponsored RadioLab podcast episode in June 2015.[158] I have not come across any academic articles addressing WAPS specifically prior to the Reel article. Holland Michel highlighted Reel's article as the first widely distributed publication about domestic WAPS. Based mainly on Reel's article, the law review articles by John Pavletic and Andrea Carlson provided an introductory analysis of Fourth Amendment jurisprudence at the time.

Following Holland Michel and *LBS v. Baltimore*, the publicly available details about WAPS were made more available for much more robust analysis and public discussions about this new technology. Although the technology presents novel questions, numerous similar circumstances have applied the Fourth Amendment to narrow the range of interpretations likely to result from the use of WAPS. Judge Ginsburg's embrace of the Mosaic Theory in *Maynard* and the subsequent concurring opinions embracing other forms of Mosaic Theory in *Jones* were scholastically significant triggers to the development in Fourth Amendment jurisprudence concerning emerging technologies, WAPS included. Although the majority opinion of *Jones* avoided the subject, several notable scholars developed legal theories better tailored to mosaic's shortfalls, and the continued expansion technology has had in law enforcement.

In "The Fourth Amendment in the Age of Persistent Aerial Surveillance," Pavletic provides a constitutional analysis of Baltimore's 2016 WAPS pilot program.[159] The analysis was largely based on Reel's article, the Flyover Cases, Circuit Courts of Appeals cases, and an explicit embrace of the Mosaic Theory. Pavletic equated WAPS to persistent GPS surveillance,

---

[157] Monte Reel, "Secret Cameras Recording Baltimore's Every Move from Above," Bloomberg Businessweek, August 23, 2016, https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ accessed July 21, 2020.
[158] Manoush Zomorodi, "Eye in the Sky," RadioLab, June 18, 2015, https://www.wnycstudios.org/podcasts/radiolab/articles/eye-sky accessed July 21, 2020.
[159] John Pavletic, *The Fourth Amendment in the Age of Persistent Aerial Surveillance*, 108 J. Crim. L. & Criminology 171 (2018). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4 accessed June 21, 2020.

according to the definition established in *Maynard*.[160] To prove this argument, Pavletic primarily relies upon the five-Justice concurrence in *Jones* and two Appeals Court decisions to endorse Mosaic Theory as a means to rule against WAPS. Pavletic acknowledged that the *Jones* majority did not accept the "long-term, continuous surveillance" aspect of the reasonable expectation of privacy.[161] In *Cuevas-Sanchez*, the Fifth Circuit Court of Appeals questioned extending *Ciraolo's* flyover against installing a pole camera on public property to look down into his backyard for thirty days.[162] The Court ruled that the camera used in that manner was a search but within the scope of the warrant to uphold the conviction. The Court ruled *Ciraolo* inadequate for *Cuevas-Sanchez* because,

> "It is not a one-time overhead flight or a glance over the fence by a passer-by. Here the government placed a video camera that allowed them to record all activity in Cuevas's backyard. It does not follow that Ciraolo authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible."[163]

Pavletic then turned to *United States v. Nerber* from the Ninth Circuit Court of Appeals.[164] *Nerber* is emphasized for its description of the invasive nature of video surveillance, "The sweeping, indiscriminate manner in which video surveillance can intrude upon us, regardless of where we are, dictates that its use be approved only in limited circumstances."[165] Like the Court,

---

[160] John Pavletic, *The Fourth Amendment in the Age of Persistent Aerial Surveillance*, 108 J. Crim. L. & Criminology 171 (2018). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4 accessed June 21, 2020, 187.

[161] John Pavletic, *The Fourth Amendment in the Age of Persistent Aerial Surveillance*, 108 J. Crim. L. & Criminology 171 (2018). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4 accessed June 21, 2020, 186-187.

[162] *United States v. Cuevas-Sanchez*, 821 F.2d 248, 1987 U.S. App. LEXIS 9524 (United States Court of Appeals for the Fifth Circuit June 29, 1987). https://advance-lexis-com.ccl.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:3S4X-93P0-001B-K2HV-00000-00&context=1516831

[163] *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251, 1987 U.S. App. LEXIS 9524, *7 (5th Cir. Tex. June 29, 1987)

[164] *United States v. Nerber*, 222 F.3d 597, 2000 U.S. App. LEXIS 21405, 2000 Cal. Daily Op. Service 7123 (United States Court of Appeals for the Ninth Circuit August 24, 2000, Filed). https://advance-lexis-com.ccl.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:4124-05T0-0038-X3Y3-00000-00&context=1516831

[165] *United States v. Nerber*, 222 F.3d 597, 603, 2000 U.S. App. LEXIS 21405, *16, 2000 Cal. Daily Op. Service 7123 (9th Cir. Wash. August 24, 2000), https://advance-lexis-com.ccl.idm.oclc.org/api/document/collection/cases/id/4124-05T0-0038-X3Y3-00000-00?page=603&reporter=1107&cite=222%20F.3d%20597&context=1516831

Pavletic took significant issue with the singling out of an individual under a mass surveillance scheme. *Carpenter* was just granted certiorari from the Sixth Circuit Court of Appeals, in which Pavletic acknowledged but did not comment on the case's potential outcomes. On balance, Pavletic acknowledged the potential benefits of WAPS surveillance, the increased conviction rate and reliability, a deterrence effect, and public safety applications outside of law enforcement, such as traffic management.[166] However, Pavletic did not believe those benefits justified the cost to civil liberties.

Pavletic's analysis's most helpful aspect is the reliance on the Mosaic Theory to strike against WAPS. The Mosaic Theory's approach to surveillance is the cornerstone of the arguments. If the Court adopted the Mosaic Theory, WAPS is not constitutional. WAPS is probably constitutional if the Court maintains a sequential approach to the Fourth Amendment.[167] The weakness of Pavletic's analysis was two-fold. First, the information about the pilot program in 2016 was limited to news reports and investigative journalism. Pavletic did not have access to the policies and procedures used by PSS during the initial test phase. The details one might need to determine the potential constitutional violations were not included in the published articles. For example, in the 2020 AIR program, the PSS analysts were not allowed to zoom in on a location unless there was a report of one of the sanctioned crimes to investigate. It is unclear if such restrictions were in place during the 2016 test. If analysts could, at a whim, zoom in on people milling about without a report of interest, the invasion of privacy may have occurred. However, neither in 2016 nor 2020 was the resolution sufficient to identify anyone from WAPS imagery alone positively. If an unscrupulous analyst zoomed in on

[166] John Pavletic, *The Fourth Amendment in the Age of Persistent Aerial Surveillance*, 108 J. Crim. L. & Criminology 171 (2018). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4 accessed June 21, 2020, 194.
[167] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 311, 315-320 (2012), https://repository.law.umich.edu/mlr/vol111/iss3/1

unsuspecting, law-abiding citizens, nothing of any detail or note could have been witnessed.[168] This is also highlighted when the precise points trigger concern in the WAPS operations. The potential injury could not occur at the point of collection or when sensors on the aircraft were operating. The potential injury was inflicted at the analysis or dissemination stage. The Mosaic Theory can only be applied during the analysis stage and later. Second, Pavletic's legal analysis was skewed because of a lack of understanding of the technical details of the sensors, which led to a misunderstanding of the operations of this new technology. In the hypothetical GPS surveillance tracking comparison, one would have the identity of the person being tracked. Likewise, with CSLI data, personal identifying information would be known because one was accessing service provider records. Even if a disposable phone was used, identifiable metadata was specific to the particular cellular device. Compare this to the ability to track a person with WAPS; without ground surveillance cross-correlation, the identity of the person being tracked cannot be known. The cross-correlation could be from traffic cameras, CitiWatch cameras in the case of Baltimore, or any other ground-level visual surveillance.[169] If one were to rely upon WAPS only to identify a person of interest (POI), at best, it could provide an address of possible employment or residency. If the person lives or works anywhere other than a single-family residence by themselves, it would take additional information to identify the POI. In another example, Pavletic discussed the Air Force's Blue Devil Program, one of Big Safari's rapid development programs, which was deployed to Afghanistan in 2010 but did not accurately describe the unique factors to the program that distinguished it from Constant Hawk or Angel Fire. Reel's article made the same statement. Neither was accurate.[170] Pavletic's limited

[168] Craig Timberg, "New Surveillance Technology Can Track Everyone in Area for Several Hours at a Time," Washington Post (Feb. 5, 2014), accessed 28 July 2021, retrieved from 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. Accessed 28 July 2021

[169] Up to and including patrol officers following the persons of interest.

[170] John Pavletic, "The Fourth Amendment in the Age of Persistent Aerial Surveillance," 108 Journal of Criminal Law & Criminology 171 (2018),

understanding and knowledge of the operational side of WAPS contributed to the inaccurate assertion of facts. The facts of the case or the hypothetical are essential to diagnose the subject best. This information gap exposed the challenge to legal scholars, policymakers, and jurists alike when the issue is particularly technical in nature.[171] Because Pavletic conducted a weak technical analysis of the systems, it skewed the accuracy and applicability of the legal analysis.

Carlson's article, like Pavletic, introduced and relied primarily on Reel's Bloomberg article to gather facts about WAPS in Baltimore. Carlson's legal analysis did not depend on the Mosaic Theory, citing the criticisms of Orin Kerr.[172] By rejecting the Mosaic Theory, Carlson analyzed WAPS under the existing precedent, not a potential novel doctrine as Pavletic did. The bulk of the article was Carlson analyzing similar cases covered in the previous chapter.[173] In the analysis of the trespassory "pre-search"[174] approach to challenging aerial surveillance, Carlson pointed to *United States v. Causby*.[175] In *Causby*, the Court rejected the Common Law claim of "*cujus est solum ejus est usque ad coelum,"*[176] stating, "It is 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."[177] One of the critical challenges of limiting aerial surveillance via

---

https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4, 176.; Blue Devil's unique characteristics were the multiple-intelligence sensor package, whereas Angel Fire and Constant Hawk were equipped with imagery intelligence (IMINT) sensors only.

[171] *Gonzales v. Carhart*, 550 U.S. 124 (2007)(The detailed discussion between the D&E versus the D&X procedures throughout this ruling reminded many of the awkwardness that can be induced by looking to the Court to solve the most pressing concerns.)

[172] Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 184.

[173] *Katz v. United States*, 389 U.S. 347 (1967), *California v. Ciraolo*, 476 U.S. 207 (1986), *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), *Florida v. Riley*, 488 U.S. 445 (1989), *Kyllo v. United States*, 533 U.S. 27 (2001), *United States v. Jones*, 565 U.S. 400 (2012)

[174] Term used by Cato Institute Fellow, Jim Harper, "In an ordinary search, you have in mind what you are looking for and you go look for it. If your dog has gone missing in the woods, for example, you take your mental snapshot of the dog and you go into the woods comparing that snap shot to what you see and hear. Pre-search reverses the process. It takes a snapshot of everything in the woods so that any searcher can quickly and easily find what they later decide to look for." Reason Magazine, originally published August 30, 2016, accessed 28 July 2021, retrieved from https://www.cato.org/commentary/pre-search-coming-us-policing

[175] *United States v. Causby*, 328 U.S. 256 (1946)

[176] Literal translation "whoever owns land it is theirs up to the heavens and down to hell"

[177] *United States v. Causby*, 328 U.S. 256, 260-261 (1946)

constitutional means is not limiting other forms of air travel over the same space. If aircraft can fly over private and public property without incident, so too could aircraft equipped with cameras. As *Knotts* reminds us, “Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case” for “a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”[178] Because Carlson focused analysis on the Flyover Cases, “precedent allows law enforcement to utilize aerial surveillance relatively unrestricted even above private property. Presently, no court in the United States has held the use of video cameras by law enforcement to survey activity on public property to be an unreasonable search.”[179] Ultimately, Carlson promoted the part of Justice Alito’s *Jones* concurrence, which many legal scholars have ignored, “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”[180] Carlson concluded that the best course of action to protect the sense of privacy many people may feel challenged was through legislative action.

According to Carlson, lawmakers should apply Gregory McNeal’s model of UAS law and policy to WAPS.[181] Because domestic commercial WAPS is operated from fixed-wing manned aircraft, the airframe is of little consequence to the Fourth Amendment. The sensor payload which collects the data is at issue. The issue of a state or locality fielding a UAS with WAPS cameras would be fiscal more than technical or legal. Whether the technology at issue is UAS

---

[178] *United States v. Knotts*, 460 U.S. 279, 281-282 (1983)

[179] Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 167-196.

[180] *United States v. Jones*, 565 U.S. 400, 429 (2012) citing Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801, 850–851(2004).

[181] Andrea Carlson, 187.; Gregory S. McNeal, “Government-Operated Drones and Data Retention,” 72 Washington & Lee Law Review 1139 (2015), https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/3; Gregory S. McNeal, “Drones and Aerial Surveillance: Considerations for Legislators” (November 11, 2014). Brookings Institution: The Robots Are Coming: The Project on Civilian Robotics, November 2014, Pepperdine University Legal Studies Research Paper No. 2015/3, https://ssrn.com/abstract=2523041

or WAPS, Carlson, and McNeal believe legislatures are best suited to respond to new surveillance technologies.[182] As far as specific legislative suggestions, Carlson applied the recommendations McNeal had for domestic UAS surveillance for WAPS, such as: protecting property owner's airspace up to 350 feet;[183] durational limits, which could be tailored to particular types of investigations, or set when warrants are necessary for further investigations;[184] data storage and access, codifying safeguards to "detect, deter, prevent, and punish" misuse of surveillance,[185] to include data encryption.

McNeal's model was based on President Obama's Memorandum to establish UAS policy under existing federal law and regulations.[186] Though the Memorandum only applied to federal authorities, McNeal believed it served as a good framework that states could apply. Additional protective measures from the Memorandum included requirements to reassess the policies for UAS at least every three years.[187] The Memorandum also ensured that UAS could not collect Personal Identifying Information (PII) without providing those identified access or the opportunity to amend records.[188] McNeal offered a tiered system of data retention: full

---

[182] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801, 850–851(2004)

[183] Gregory S. McNeal, "Drones and Aerial Surveillance: Considerations for Legislators" (November 11, 2014). Brookings Institution: The Robots Are Coming: The Project on Civilian Robotics, November 2014, Pepperdine University Legal Studies Research Paper No. 2015/3, https://ssrn.com/abstract=2523041

[184] As applied to WAPS, legislation could specify the conditions which investigators or analysts could zoom in to view specific individuals or locations.

[185] Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 192.

[186] Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, White House, § 2(b) (Feb. 15, 2015), accessed 28 July 2021, retrieved from https://www.govinfo.gov/content/pkg/DCPD-201500103/pdf/DCPD-201500103.pdf

[187] Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, White House, § 2(b) (Feb. 15, 2015), accessed 28 July 2021, retrieved from https://www.govinfo.gov/content/pkg/DCPD-201500103/pdf/DCPD-201500103.pdf, 3.

[188] Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, White House, § 2(b) (Feb. 15, 2015), accessed 28 July 2021, retrieved from https://www.govinfo.gov/content/pkg/DCPD-201500103/pdf/DCPD-201500103.pdf, 4. ("Personally identifiable information" refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, as set forth in Office of Management and Budget Memorandum

accessibility for 30 days, to include near real-time or forensic analysis; after 30 days, the data should be moved to servers accessible only with a court order and probable cause; after 90 days, a court order and probable cause that the information contains evidence of a crime; all data on the servers should be deleted after as early as 120 days but no more than five years.[189] These legislative suggestions are one set of potential remedies that can address how WAPS could be reasonable.

Carlson or Pavletic's articles did not settle the constitutional standing of WAPS. Carlson's analysis of WAPS was published the same year as Pavletic demonstrated a more thorough legal and scholarly analysis of Fourth Amendment jurisprudence at the time, which led to the opposite conclusion. These earnest assessments demonstrate why this study is necessary, not to repeat Carlson or Pavletic, but to provide the best analysis available to what is likely to be a ripe legal, political, and social challenge in the future of acceptable surveillance techniques and technologies. Neither Pavletic nor Carlson was able to include an analysis of *Carpenter*. Both were published in 2018. Since 2018, there have been no legal articles specifically addressing WAPS until Ferguson's 2022 forthcoming article, *Persistent Surveillance*.[190] Pavletic and Carlson were law students at the time of publication. Carlson has since graduated and is in private practice. Pavletic is a Federal Judicial Law Clerk. There are no indications of additional WAPS scholarship by either author. As of August 2021, Pavletic's article has been cited five times. Carlson's article has been cited once. In conjunction with Reel's article, Bloomberg QuickTake Originals made a short video interviewing McNutt and describing WAPS; it has fewer than 25,000 views.[191] Metrics were not available from RadioLab

M–07–16 (May 22, 2007) and Office of Management and Budget Memorandum M–10–23 (June 25, 2010).")

[189] Gregory S. McNeal, "Government-Operated Drones and Data Retention," 72 Washington & Lee Law Review 1139 (2015), https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/3, 1150.

[190] Andrew Guthrie Ferguson, "Persistent Surveillance" (June 10, 2022), Alabama Law Review, Forthcoming, https://ssrn.com/abstract=4071189

[191] "The Surveillance Firm Recording Crimes From Baltimore's Skies," Bloomberg Quick Take Originals https://youtu.be/wRa-AucbN6k, September 1, 2016, accessed July 20, 2020.

of the reception of their WAPS episode. Much more development is necessary for the substantive discussions surrounding WAPS for domestic use.

Legal scholarship addressing WAPS remains limited; however, the scholarship about the doctrines introduced in the previous chapter is abundant and robust. This next section will provide a literature review of scholarship on the most pressing doctrines from *Kyllo* to the present.[192] Though WAPS was still in the laboratory at the time of *Kyllo*, the manner in which the Court addressed emerging technology set the trajectory for legal scholars to formulate doctrines and theories for the twenty-first century. Orin Kerr is the most significant Fourth Amendment scholar skeptical of any of the Mosaic Theories or new approaches to the Fourth Amendment.[193] Kerr was cited in *Carpenter* nine times across the four different dissenting opinions.[194] In *Riley v. California*, a case in which the Court ruled a warrant is necessary to search a phone, Kerr was cited twice.[195] In *Jones*, Kerr was cited three times.[196] There is no other contemporary of Kerr whom the Court consistently looks to on matters of technology and the Fourth Amendment. Kerr has not published any analysis of WAPS beyond a Tweet thread in response to the Fourth Circuit en banc decision. Kerr concluded his assessment of the decision, saying, “I am kind of amazed that this sort of reasoning is in the name of the 4th Amendment, as it seems so far

---

[192] *Kyllo v. United States*, 533 U.S. 27 (2001)

[193] Orin Kerr was a Law Clerk under Justice Kennedy in 2003, he is Professor of Law at UC Berkley School of Law. He was previously the Frances R. and John J. Duggan Distinguished Professor of Law at University of Southern California Gould School of Law, his honors include “#1 most-cited U.S. law professor in Criminal Law and Procedure” from 2013-17 and 2016-2020 according to Leiter Rankings; Orin Kerr, “Do We Need a New Fourth Amendment?,” 107 Michigan Law Review 951 (2009), https://repository.law.umich.edu/mlr/vol107/iss6/5

[194] The articles by Kerr cited in *Carpenter* dissents: Orin Kerr, “The Mosaic Theory of the Fourth Amendment,” 111 Michigan Law Review 311 (2012). https://repository.law.umich.edu/mlr/vol111/iss3/1; “An Equilibrium-Adjustment Theory of the Fourth Amendment,” 125 Harvard Law Review 476, 113-134 (2011); “Katz Has Only One Step: The Irrelevance of Subjective Expectations,” 82 University of Chicago Law Review 113 (2015), accessed July 21, 2020, https://lawreview.uchicago.edu/publication/katz-has-only-one-step-irrelevance-subjective-expectations-0#; “Four Models of Fourth Amendment Protection,” 60 Stanford Law Review 503, 505 (2007); “The Case for the Third-Party Doctrine,” 107 Michigan Law Review 561, 563, n. 5, 564 (2009).

[195] *Riley v. California*, 573 U.S. 373 (2014)

[196] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801, 816 (2004) accessed July 21 2020, https://repository.law.umich.edu/mlr/vol102/iss5/1/

removed from the kind of analytical steps that you normally consider. But I guess every day is a new day in the world of the Mosaic Theory."[197] Kerr has numerous articles which contribute to a necessary understanding of the Fourth Amendment and its interaction with new technology. Kerr's lack of attention to WAPS provides room for development in Fourth Amendment analysis. His analysis of the Court's approaches to the Fourth Amendment has largely been observational compared to his contemporaries, who offer prescriptive suggestions for a proactive judiciary to resolve the concerns between technology and the Fourth Amendment. Kerr has consistently emphasized the importance of legislatures as the fittest bodies to regulate the technology and privacy balance.[198] He essentially stands alone in the sphere of legal scholars who also write about the intersection of law and technology.[199]

---

[197] Orin Kerr, @OrinKerr, 10:53am, Jun 24, 2021 https://twitter.com/orinkerr/status/1408121033320771587?lang=en; https://twitter.com/OrinKerr/status/1408126899189075968

[198] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 311 (2012), 352, https://repository.law.umich.edu/mlr/vol111/iss3/1

[199] In "The Fourth Amendment and the New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), Kerr lists some of the scholars who disagree with him, to include Lawrence Lessig, Lawrence Tribe, and Michael Adler; Note, "Cyberspace, General Searches, and Digital Contraband: the Fourth Amendment and the Net- Wide Search," 105 Yale Law Journal 1093 (1996) (arguing that current Fourth Amendment doctrine gives the government too much power to use new technologies in ways that erode privacy, and that the doctrine should be reevaluated to better protect privacy); Marc Jonathan Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity," 82 Texas Law Review 1349, 1363 (2004) (contending that the scope of the Fourth Amendment protection "needs rethinking if constitutional privacy protections are to work well in twentyfirst century conditions."); Morgan Cloud, "Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment," 72 Mississippi Law Journal 5, 49 (2002) (arguing that the Supreme Court should respond to the problem of new technologies by "enunciat[ing] an expansive, value-based theory of the scope of the Fourth Amendment and its role in preserving privacy and liberty"); Melvin Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance," 39 Syracuse Law Review 647, 650 (1988) (arguing that recent cases "fail[] to protect privacy rights, and permits their gradual decay with each improved technological advance"); Roberto Iraola, "New Detection Technologies and the Fourth Amendment," 47 South Dakota Law Review 8 (2002) (arguing that the Fourth Amendment should regulate the use of detection technologies); Tracey Maclin, "Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century," 72 Mississippi Law Journal 51, 51 (2002) (contending that as technology advances and allows greater means to invade privacy, the Courts should interpret the Fourth Amendment such that "the privacy and security protected by the Fourth Amendment should not depend on innovations in technology"); Raymond Shih Ray Ku, "The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance," 86 Minnesota Law Review 1325 (2002) (arguing that the Fourth Amendment should be interpreted to require legislative authorization of government use of new technologies to better protect privacy against new technologies); Ric Simmons, "From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century

Kerr's has spent over a decade describing the jurisprudential temperament of the Fourth Amendment. Beginning with "The Fourth Amendment and the New Technologies: Constitutional Myths and the Case for Caution," building upon his evaluation of it in "The Four Models of Fourth Amendment Protection," culminating in "An Equilibrium Adjustment Model of the Fourth Amendment," which continues to be applied to the more recent case studies exemplified in "Implementing Carpenter" and "The Questionable Objectivity of the Fourth Amendment."[200] This chapter will analyze Kerr's observations of the Court's jurisprudence and will engage with his critics. This chapter will also address the scholarly articles cited in the Fourth Circuit's rulings, none of which directly address WAPS but laid Fourth Amendment principles that contributed to

---

Technologies," 53 Hastings Law Journal 1303 (2002) (arguing that courts should focus on the result of a search on privacy interest rather than the means of its invasion in order to guarantee robust Fourth Amendment protection in new technologies); David A. Sklansky, "Back to the Future: Kyllo, Katz, and Common Law," 72 Mississippi Law Journal 143, 210 (2002) (suggesting that "Kyllo is a promising decision" because it recognizes "the ways in which new technology can erode a traditional sphere of privacy" and also is sensitive to "the past, present, and the future"); Christopher Slobogin, "Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance," 86 Minnesota Law Review 1393, 1411 (2002) (arguing that Kyllo is insufficiently protective of privacy and that " [m]embers of our society should be constitutionally entitled to expect that government will refrain from any spying on the home - technological or otherwise - unless it can demonstrate good cause for doing so"); Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 S. California Law Review 1083, 1087 (2002) (arguing that Fourth Amendment doctrine does not protect privacy sufficiently against new technologies, and that Fourth Amendment law should create an "architecture of power" to maintain an appropriate balance of power among individuals, institutions, and the government in light of "the ever-increasing data flows of the Information Age"); David E. Steinberg, "Making Sense of Sense-Enhanced Searches," 74 Minnesota Law Review 563, 629 (1990) (arguing that "[n]owhere is an appropriate application of the warrant clause more essential to protect the security promised by the fourth amendment" than in the case of sense-enhancing technologies); Andrew E. Taslitz, "The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions," 65 Law & Contemporary Problems, Spring 2002, at 125, 131 (arguing that Fourth Amendment protections should be expanded "by redefining privacy from the primarily cognitive to the primarily affective," and that "[p]rivacy in the information age is best conceived as the maintenance of metaphorical boundaries that define the contours of personal identity"); James J. Tomkovicz, "Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures," 72 Mississippi Law Journal 317, 438 (2002) (arguing that in order to protect privacy from the threat of new technologies, "[o]fficial exploitation of a scientific or technological device should be considered a Fourth Amendment search").

[200] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004); "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296; Orin Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011), 476-543, accessed July 21, 2021, https://ssrn.com/abstract=1748222; Orin Kerr, "Implementing Carpenter" *The Digital Fourth Amendment* (Oxford University Press), Forthcoming, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257; Orin Kerr, "The Questionable Objectivity of Fourth Amendment Law," 99 Texas Law Review 447 (2021), 447-489, accessed July 13, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3651475

the opinions.[201] The most notable critics of Kerr are David Gray, Danielle Citron, and Christopher Slobogin. None of these scholars have published an article specifically addressing WAPS. They have continued to develop different forms of mosaic theories or changes to aggregated approaches to Fourth Amendment analysis versus Kerr's emphasis on maintaining a sequential approach to Fourth Amendment jurisprudence. Most Fourth Amendment legal scholarship has focused on the digital realm of Big Data, cloud drives, drones, active location tracking, facial recognition, license plate readers, and the sort. Quantitatively speaking, there is far less constitutional skepticism specifically concerned with widespread camera-based dragnets as what is presented in WAPS.

Kerr is a pragmatist. "The Fourth Amendment and the New Technologies: Constitutional Myths and the Case for Caution" argues against the "popular view" amongst Fourth Amendment scholars. The "popular view" was defined as "The view that the Fourth Amendment should be interpreted broadly in response to technological change,"[202] how this practically operated, the "Courts should take the lead crafting rules to protect privacy because courts are well-situated to regulate criminal investigations involving new technologies."[203] Kerr critiqued the popular view on its "inaccurate view of Fourth Amendment doctrine, history, and function." Which he believed is a cautionary tale more than an encouragement for "an aggressive judicial role in the application of the Fourth Amendment to developing technologies."[204] Kerr argued that legislatures are better equipped to respond to paradigm shifts caused by new technologies. Each time there was a shift caused by disruptive technology, an equilibrium was found. For

[201] Barry Friedman, "Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program," New York University Policing Project, November 2020, https://www.policingproject.org/air accessed June 16, 2022.;
[202] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 804.
[203] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 805.
[204] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 805.

Kerr, that equilibrium was best identified and employed by representative bodies. Legislatures are and have been better situated than courts to these tasks because "legislative predominance in the face of developing technologies is consistent with current Fourth Amendment doctrine, accurately reflects historical practice, and is likely to continue in the future given the relative institutional competence of courts and legislatures."[205] The novel characteristics of new technologies have the potential to grow so rapidly, that if the courts take the lead, their "institutional limits" might be exposed in attempts to adapt to rapidly changing technology. For some points of reference, in 2004, the Motorola Razr was the sleek new phone, Youtube would appear a year later, and Facebook had just been incorporated, two years before it would be open to the public. The technological innovations which have set the norms of the present generation were in their infancy. Kerr challenged the popular view from a doctrinal approach which disputed the necessity of the courts to lead in the protection of privacy from new technologies.

Kerr defended this argument in three parts. The first explained why the court took an active role in determining privacy and technology cases—the close tie between privacy interests and property rights.[206] The legal sanctity of a person's home is paramount, not necessarily because of the Fourth Amendment to the Courts, but because of property rights. For instance, not only were homes protected, but so too were rental spaces,[207] storage lockers, and "closed containers," which include physical and digital files. Kerr next used the model of *Olmstead* and wiretapping to demonstrate the fitness of the legislative bodies over the judicial bodies. *Olmstead v. United States* is a 1928 case in which the Court ruled warrantless wire-tapping conducted during a Prohibition investigation was not a search or seizure.[208] However, at the

[205] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 806.
[206] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 809.
[207] As long as the rental contract is being honored and payments are current.
[208] *Olmstead v. United States*, 277 U.S. 438 (1928)

time, more than half the states already had statutory bans on wiretapping.[209] By 1934, Congress passed the Communications Act, which also prohibited wiretapping.[210] This reaction was not a one-off. In *Berger v. New York*, the Court formulated five conditions necessary for wiretapping to be constitutional.[211] The Federal Wire Interception Act was introduced to the Senate at the same time as *Berger* was being considered. Two weeks after *Berger*, the Electronic Surveillance Control Act was introduced to codify the five conditions listed in *Berger*. Congress combined the two and passed the Federal Wiretap Act in 1968, which is colloquially known as Title III.

Congress continued to intervene on the people's behalf following additional Court rulings striking against privacy. Following *Smith v. Maryland,* where the Third Party doctrine was applied to telephone company pen registers, Congress passed the Pen Register and Trap and Trace Devices Statute.[212] The Privacy Act of 1974 authorized citizens to access and correct information about themselves in government computer databases. The Cable Communications Act of 1984 prohibited the disclosure of cable subscribers' personal information. The Electronic Communications Privacy Act of 1986 protected stored emails and internet communications. According to Kerr, each of these legislative acts demonstrated the appropriateness of legislatures to play the active role in protecting the people's privacy rather than the Courts. The final argument Kerr presented was the institutional limits of the courts versus legislatures to make adaptable responses to rapidly changing technologies. This section challenged Lawrence Lessig's *Code and Our Other Laws of Cyberspace*, where Lessig argued, "judges should firmly advance arguments that seek to preserve original values of liberty in a new context."[213]

---

[209] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 841.
[210] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 845.
[211] *Berger v. New York*, 388 U.S. 41 (1967)
[212] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 855. Citing 18 U.S.C. §§ 3121-27 (2000).
[213] Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004), 858.

According to Kerr, Lessig argued if courts deferred to legislatures, “we will be left with laws that may or may not respect constitutional values.” The primary limitation of courts Kerr pointed to was the difficulty for judges to “fashion lasting guidance when technologies are new and rapidly changing.”[214] Kerr also appealed to the design of the courts as being too inflexible to sufficiently test their new rules and approaches before they become outdated. Kerr concluded the article by noting the pattern and trajectory of the courts’ active roles flowed from the Warren Court, which “reflect[ed] the best of what criminal procedure should be.”[215] However, the Courts are not the best-suited institution for the rapid, complex responses necessary to respond to challenges presented in modern criminal procedure and new technologies.

Speaking of rapid, complex responses to new technology, WAPS is an exemplar case. The technology is not particularly new; however, the processing capabilities appear to be the concerning factor. Kerr would likely advocate that WAPS be addressed by state and local bodies instead of courts because of the additional complexities in each potential locale. For example, Baltimore's AIR program was under particular scrutiny because of its poor history, including federal consent decrees and state oversight of the Baltimore Police Department. The BPD’s willingness to deploy the precursor to the AIR program in 2016 while purposefully hiding it from the public and any elected officials complicated the individual case and application of WAPS. Those initial actions directly contributed to several of the factors in the AIR program’s Memorandum of Understanding, which arguably made more strict conditions on the WAPS system, limiting the program’s success while stoking additional concerns from those skeptical of Baltimore’s policing. These factors lead to significant considerations in the federal courts. For example, the AIR program could have had infrared coverage during periods of darkness, but the program was only approved for daytime surveillance. The preliminary Rand Corporation report

[214] Orin Kerr, “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,” 102 Michigan Law Review 801 (2004), 858.
[215] Orin Kerr, “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,” 102 Michigan Law Review 801 (2004), 887.

on the effectiveness of the AIR program highlighted that limitation as a factor limiting the success of the program because fewer homicides were committed during daylight hours than at night. Likewise, there was an expectation that the WAPS data would be shared with defense councils in criminal cases using WAPS, but no such data was turned over in the months the AIR program operated. Suppose other jurisdictions deploy WAPS systems with different ground-level surveillance assets for longer/shorter periods of time, using infrared cameras and tracking different suspected crimes. In that case, the factors on which the Fourth Circuit based its judgment could be easily inapplicable.

To further complicate matters, the Court has not consistently defined the "reasonable expectation of privacy." Kerr believes no single model can accurately and consistently be applied to the various cases of police practices. In "The Four Models of Fourth Amendment Protection," Kerr identified the coexisting models of probability, private facts, positive law, and policy models courts can use depending on the particulars of each case.[216] Much hinges on whether or not a police practice is reasonable or not. If the act is reasonable, the evidence gained is admissible; if not, it must be excluded. Excluded evidence in criminal law frequently leads to mistrials or acquittals. The cost then of improperly searching is high. Kerr was mainly concerned with the ability of trial courts to apply clear rules in the myriad of cases they will have. The primary advantage of acknowledging the four different models against a single model is the decentralization of the Fourth Amendment, again to the benefit of the lower courts, who must apply the methods of the higher courts. It is important to introduce the different models to show the interconnectedness and complexity of Fourth Amendment interpretation and application.

The Probabilistic Model is a descriptive assessment based on where the individual is and the prevailing social practices at the time of interest.[217] The probabilistic model was

[216] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021.
[217] *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978), Rakas denied a reasonable expectation of privacy for passengers in a vehicle they did not own. The petitioners were in the vehicle pulled over following a

exercised in *Bond*, *Ciraolo*, and *Olson*.[218] In *Bond*, the court rejected a Border Patrol agent feeling the contents of the petitioner's bag on a bus. In *Olson*, the court rejected a warrantless arrest absent exigent circumstances while he was an overnight guest. The Fourth Amendment sanctity of the home was not limited only to the homeowners. On the other hand, the Probabilistic Model was not used in *Illinois v. Caballes* or *United States v. Miller*.[219] *Caballes* upheld a warrantless drug-sniffing dog during a traffic stop for speeding. *Miller* applied the Third Party doctrine to bank records which were used to convict him of conspiracy in an unregulated distillery. In each of the applied cases, Kerr argued, the reasonable expectation of privacy was a descriptive expectation based on norms and prevailing social conventions which were deemed hypothetically reasonable by a reasonable person.[220]

The Private Facts model was more concerned with what information was collected than how it was collected. The examples used to describe this model were *United States v. Jacobsen*, *Dow Chemical Company v. United States*, and *United States v. Karo*.[221] In *Jacobsen*, white powder seeped out of the package during a UPS delivery. An FBI agent administered a field test for cocaine, which was positive. The question before the Court was if the test was reasonable. The test only identified the substance outside the package, incident to a crime. In *Dow Chemical*, the Court did not believe the aerial photography revealed "intimate details,"[222] therefore it was not a search.[223] In *Karo,* a case similar to *Knotts*, the use of a tracking device in a can of chemicals used for illegal narcotics. However, in this case, the tracking device was

---

robbery report. To assert Fourth Amendment protection the petitioners must have standing, the rights may not be "vicariously asserted."

[218] *Bond v. United States*, 529 U.S. 334 (2000); *California v. Ciraolo*, 476 U.S. 207 (1986); *Minnesota v. Olson 495 U.S. 91 (1990)*.

[219] *Illinois v. Caballes*, 543 U.S. 405 (2005); *United States v. Miller*, 425 U.S. 435 (1976)

[220] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 510.

[221] *United States v. Jacobsen*, 466 U.S. 109 (1984); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986); *United States v. Karo*, 468 U.S. 705 (1984)

[222] *Dow Chemical Co. v. United States*, 476 U.S. 227, 238 (1986).

[223] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 513.

used to identify the can's location inside a private home. By revealing information about the "interior of the premises…[which] could not have otherwise been obtained without a warrant," [224] the search was unreasonable. The counter-example Kerr highlighted was *Arizona v. Hicks*.[225] In *Hicks*, subject to an investigation of gunfire in an apartment complex, an officer noticed expensive audio equipment amidst a disheveled apartment. The officer diverted his attention to the equipment and moved it to read the serial number. The equipment was stolen; however, the Court ruled that the movement to ascertain the status of that equipment was an illegal search.

The Positive Law model depended if the government committed a prohibited act other than the potential Fourth Amendment violation. As with the other models, this was also more descriptive than normative. Kerr used *Rakas v. Illinois*, *Florida v. Riley*, and Justice Powell's dissent in *Dow Chemical* to illustrate this model.[226] *Rakas* denied the property right, specifically the right of vehicle passengers to refuse a search.[227] In *Riley*, the Court's opinion relied on the FAA's altitude safety regulations which allowed them to fly over the rural property and search without it being an unreasonable search. Justice White's concurrence in the plural opinion articulated the positive law model saying, "We would have a different case if flying at that altitude had been contrary to law or regulation."[228] Therefore, because the police did not commit a prohibited act prior to the search, the search was reasonable. Counter-examples to the positive law model were the Open Fields doctrine in its entirety. *Oliver v. United States*, which affirmed the Open Fields doctrine established by *Hester v. United States* to be consistent with *Katz v. United States*, expressly rejected the positive law model.[229] However, in *Greenwood v.*

---

[224] *United States v. Karo*, 468 U.S. 705, 715 (1984).
[225] *Arizona v. Hicks*, 480 U.S. 321 (1987).
[226] *Rakas v. Illinois*, 439 U.S. 128 (1978); *Florida v. Riley*, 488 U.S. 445 (1989); *Dow Chemical Co. v. United States*, 476 U.S. 227, 240-252 (1986).
[227] *Rakas v. Illinois*, 439 U.S. 128, 148 (1978)
[228] *Florida v. Riley*, 488 U.S. 445, 451 (1989) (White, J., plurality opinion, joined by Rehnquist, C.J., Scalia, J., and Kennedy, J.).
[229] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 518. Citing *Oliver v. United States*, 466 U.S. 170, 183-184 (1984).

California, the Court disregarded California's constitutional law in exchange for "our societal understanding that certain areas deserve the most scrupulous protection from government invasion."[230]

The Policy model was based on normative value judgments to determine whether particular practices were reasonable. The Policy model asked if particular law enforcement practices were regulated by the warrant requirement or unleashed by the Fourth Amendment. If the conduct in question became troublesome to civil liberties, it was a violation; if the result was too great a restriction on investigative abilities, it was not a violation.[231] Kerr believed this model was practiced even though cases were framed under the other three models. The best example was *Katz* itself. The Court based its justification on the sanctity of the public phone booth providing a reasonable expectation of privacy because of "the vital role that the public telephone has come to play in private communication."[232] *Kyllo* was another example. Justice Scalia took on a "long view" of concern against "sense-enhancing technology," which could obtain "information regarding the interior of a home that could not otherwise have been obtained without physical intrusion"[233] The counter-example to the policy model was exemplified in *Palmer v. Hudson* where the court denied an incarcerated inmate any expectation of privacy in his cell because the "recognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions."[234] The Policy model's weakness was the inability to be consistent. A specific

---

[230] *California v. Greenwood*, 486 U.S. 35, 43 (1988)
[231] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 519.
[232] *Katz v. United States*, 389 U.S. 347, 352 (1967)
[233] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 520. Citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001)
[234] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 521. Citing *Palmer v. Hudson*, 468 U.S. 517, 526 (1984).

policing practice could always be defined as more broad or narrow.[235] The reliance interests of the lower courts was a compelling stopgap; there are over eight hundred thousand law enforcement officers with the power of arrest and eight million government employees subject to the Fourth Amendment.[236] An inconsistent rule spread that far can easily become a hydra of a policy.

The analysis of the four models delineated them between micro and macro in scale and normative and descriptive axes. Because the models shared at least one characteristic with another model, they frequently overlap. The difficulty in applying the "reasonable expectation of privacy" doctrine is in the consequences of the exclusionary rule applied when police practices go too far. The doctrine must be comprehensible for law enforcement officers. However, because of the complex nature of the range of conditions that may or may not trigger doctrinal limitations, Kerr advocated the four models against any single model. Kerr did not believe a single approach could thread the proverbial needle as well as the models he observed. The inadequacy of any single model or the four models is most useful in leading readers to Kerr's Equilibrium Adjustment Model, which has been more helpful than the other four.[237] Developing these four models was important to show the interconnectedness and complexity of Fourth Amendment jurisprudence.

Kerr amended his arguments from the Four Models in 2011 to create his current model, the Equilibrium-Adjustment model. This single model posited that as new technologies or social practices change the status quo of the Fourth Amendment, the Court expands or contracts the government's power against constitutional protections. Kerr believed this model explained

---

[235] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 539.
[236] Orin Kerr, "Four Models of Fourth Amendment Protection," 60 Stanford Law Review 503 (2007), https://ssrn.com/abstract=976296 accessed May 20, 2021, 537.
[237] Orin Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011), https://harvardlawreview.org/wp-content/uploads/pdfs/vol125_kerr.pdf accessed July 21, 2020.

decades of Fourth Amendment jurisprudence and balancing tests demonstrated when the courts addressed vehicle exceptions and sense-enhancing devices and reduced the use of the mere evidence rule,[238] telephone networks, undercover investigations, aerial surveillance, subpoenas, and the special protections for the home. The Equilibrium-Adjustment model was necessary. As new technologies and techniques have been introduced into investigative practices, criminal behavior has adapted from law enforcement practices. Jurists have then accounted for the changed conditions in an attempt to balance police power against the new norms and social practices. The constant expansion and contracting of the Fourth Amendment have been intended to maintain stability within the broader search and seizure doctrine.[239]

For the expanding and contracting of Fourth Amendment jurisprudence to be successful, the Court must delay or bind the new restrictions to a time period to provide the space for evolution to stabilize the forces in competition with one another. After relative stability has been established, the Court could establish new rules. This chain of events is why the Court tends to wait until a new technology has found its equilibrium within a given society. Kerr has been careful to account for the goals of the Court; the practices are not always as ideal.[240] This model is like the common law; both adjust the relationship according to societal changes. The common law seeks to keep up with "felt necessities of the time, the prevalent moral and political theories, [and] intuitions of public policy, avowed or unconscious."[241] This model is distinct from the

[238] Doctrine developed from *Boyd v. United States*, 116 U.S. 616 (1886), which the Court ruled a statute cannot require production of records which can be used as incriminating evidence.
[239] Orin Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011), https://harvardlawreview.org/wp-content/uploads/pdfs/vol125_kerr.pdf accessed July 21, 2020, 481-483.
[240] Orin Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011), https://harvardlawreview.org/wp-content/uploads/pdfs/vol125_kerr.pdf accessed July 21, 2020, 488
[241] Orin Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011), https://harvardlawreview.org/wp-content/uploads/pdfs/vol125_kerr.pdf accessed July 21, 2020, 492.

common law for its persistently defensive posture that does not try to keep up with society's evolving standards. It aims to maintain the status quo amidst technological and social changes.

To support the Equilibrium-Adjustment model, Kerr hypothesized eight examples to demonstrate it being applied. The interest of this study is how the model is applied to aerial surveillance. In *Ciraolo*, the court did not believe officers had “to shield their eyes when passing by a home on public thoroughfares” regardless of where the public thoroughfares were located on the ground or one thousand feet in the air.[242] One might have expected the court to interpret the additional interior raised fence in the curtilage to assert an “expectation be one that society is prepared to recognize as "reasonable."[243] However, under the Open Fields doctrine, additional fences around the property but not to a home do not create a closed field.[244] The work of the model showed how fences could not be used to demonstrate Fourth Amendment protection. It does not yet hypothesize how more advanced aerial surveillance platforms would interact with it. The model was not predictive like the four previous models suggested; Equilibrium Adjustment is a descriptive normative model. As applied to *Ciraolo*, the purpose was not to endorse passion-driven jurisprudence as a punctuated reaction but instead to let legislatures and time work out the equilibrium and let the courts acknowledge when the equilibrium has been reached.

The following year, the Court ruled on *United States v. Jones.*[245] The five-Justice embrace of two different kinds of Mosaic Theory caused a stir among Fourth Amendment scholars. To Kerr, it posed a disturbing suggestion to Fourth Amendment paradigms. In response, Kerr presented a strong defense for the traditional sequential approach to the Fourth

---

[242] Orin Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," 125 Harvard Law Review 476 (2011), https://harvardlawreview.org/wp-content/uploads/pdfs/vol125_kerr.pdf accessed July 21, 2020, 524.
[243] *Katz v. United States*, 389 U.S. 347, 361 (1967)
[244] *United States v. Dunn*, 480 U.S. 294 (1987)
[245] *United States v. Jones*, 565 U.S. 400 (2012)

Amendment.[246] If the Court were to explicitly embrace any of the Mosaic Theory versions, to Kerr, "the Mosaic Theory offers a fundamental challenge to current Fourth Amendment law."[247] As a demonstration, Kerr presented four major questions the Court would need to answer if the Mosaic Theory were to be accepted: "What test would determine when a mosaic has been made?" How should conduct be grouped to determine when the mosaic has crossed a line? How are mosaics to be analyzed from a reasonableness standpoint? What is the remedy for a mosaic that has crossed the line?[248] Each of these begs additional questions, where Kerr presented approximately one hundred other questions concerning how a Mosaic Theory might be implemented. Among these questions, Kerr highlighted the importance that the rules be workable at the level of the law enforcement officer, not only the courthouse. The most contentious political issues which have come before the court in major doctrinal shifts are the "reliance interests,"[249] i.e., the cost of the court taking a decisive blow to any particular doctrine. Courts tend to embrace change in a piecemeal fashion to prevent such punctuated changes. Fourth Amendment interpretation has been no different in that scheme. The pragmatism of embracing a Mosaic Theory poses significant "reliance interests" because of the jurisprudential chaos that would result from the court embracing a Mosaic Theory. Kerr argued that the Courts should reject the Mosaic Theory. This article is quintessential to any court or scholar before they advocate or embrace the Mosaic Theory. In response, Gray, Citron, and Slobogin proposed their versions of new Fourth Amendment paradigms due to the unworkability of the Mosaic Theory from *Jones*/*Maynard*. For the next six years, scholars went back and forth hypothesizing

[246] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 311 (2012), https://repository.law.umich.edu/mlr/vol111/iss3/1 accessed July 21, 2020.
[247] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 311 (2012), https://repository.law.umich.edu/mlr/vol111/iss3/1 accessed July 21, 2020, 314.
[248] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 311 (2012), https://repository.law.umich.edu/mlr/vol111/iss3/1 accessed July 21, 2020, 329.
[249] "Reliance damages," Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/wex/reliance_damages, accessed December 7, 2021.

and developing what the new Fourth Amendment might look like in the digital age until *Carpenter v. United States*.

Thus far, Kerr's equilibrium adjustment model has not been satisfactorily equilibrated or adjusted by legislatures or Courts. I concur with Kerr and Carlson; legislatures are best suited to tune the specifics of WAPS over state and local jurisdictions. In the absence of action, to even hold hearings on WAPS, the academy should present the options and conditions of satisfactory models ready for when the issue is addressed.

In *Carpenter* and *Riley v. California*, the Court stepped into the digital realm.[250] Because the digital realm is distinct from the physical, establishing a new scheme of rules was necessary. Kerr developed one suggested scheme in "Implementing Carpenter."[251] Kerr argued that the *Carpenter* rules should apply when digital records "of a kind and nature that generally could not be collected in a pre-digital age,"[252] the records were created without the "subject's meaningful voluntary voice,"[253] or the records reveal private facts, also known as personal information.[254] According to 18 U.S.C.A. § 2725 (3), personal information or personal identifying information (PII) includes a photograph, social security number, driver identification number, name, address, telephone number, and medical or disability information.[255] When all three conditions are met, precedent from *Carpenter* should protect those records. To adopt a Mosaic Theory would shift the limiting test to cases of long-term surveillance according to Justice Alito's

---

[250] *Carpenter v. United States*, 585 U. S. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014)
[251] Orin Kerr, "Implementing Carpenter," The Digital Fourth Amendment (Oxford University Press), Forthcoming, December 14, 2018, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257
[252] Orin Kerr, "Implementing Carpenter," The Digital Fourth Amendment (Oxford University Press), Forthcoming, December 14, 2018, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257, 16.
[253] Orin Kerr, "Implementing Carpenter," The Digital Fourth Amendment (Oxford University Press), Forthcoming, December 14, 2018, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257, 20.
[254] Orin Kerr, "Implementing Carpenter," The Digital Fourth Amendment (Oxford University Press), Forthcoming, December 14, 2018, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257, 22.
[255] 18 U.S.C.A. § 2725 (West)

version or to a case-by-case analysis which leads to unworkable standards reliant on endless line drawing to identify when exactly the violation was manifest.[256] Much of the criticisms of Mosaic Theory were the same challenges from his 2012 article. The significance of this article was the more recent development of the Equilibrium-Adjustment model being applied and the reiterated challenges to the Mosaic Theory. *Carpenter* did not explicitly affirm the Mosaic Theory; however, the Fourth Circuit adopted it in *Leaders of a Beautiful Struggle*. This embrace is challenging for those seeking to apply *Carpenter* to WAPS because the imagery would have to be classified in the scope of the "unique nature" of CSLI and not "conventional surveillance techniques and tools, such as security cameras."[257] Although the statutory definition of personal information includes a photograph of a person, Chief Judge Gregory did not describe the single pixel that a person appeared in the AIR program as identifying information. Instead, the Court argued that because an individual's movement could be traced to their residence, WAPS amounted to "enable[ing] deductions from the whole of individuals' movements," as the CSLI data addressed in *Carpenter*.[258]

As previously mentioned, Kerr is not without his critics.[259] Among the most substantive of those critics are; Christopher Slobogin, a law professor at Vanderbilt Law School, David Gray of Francis King Carey School of Law, and Danielle Citron of the University of Virginia School of Law. Andrew Ferguson of American University's Washington School of Law is the first law professor to publish a law review article directly addressing WAPS in a focused analysis. The two earlier law review articles responding to Reel's expose on WAPS in 2016 Baltimore by Pavletic and Carlson were written as law students. Neither has published further Fourth Amendment-related research. Slobogin has been cautious of widespread surveillance in his

---

[256] Orin Kerr, "Implementing Carpenter," The Digital Fourth Amendment (Oxford University Press), Forthcoming, December 14, 2018, USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257, 36-37.
[257] *Carpenter v. United States*, 138 U.S. 2206, 2210 (2018)
[258] *Leaders of a Beautiful Struggle v. Baltimore Police Department* (4th Cir. 2021) 2 F.4th 330, 345
[259] See Footnote 199.

publications since 2002. He and Kerr were featured in a series of short articles in the Harvard Law Review discussing Kerr's Equilibrium Adjustment theory.[260] Gray's scholarship initially focused on transitional justice. His scholarship has focused on privacy and criminal justice since 2013. Citron's scholarship has focused on sexual privacy, speech, and the digital age. Citron has been publishing privacy scholarship since 2007. All of the critics have embraced some form of a Mosaic Theory, albeit with significant adjustments in some models that they might better be framed under a different moniker.

In "Public Privacy," Slobogin argued that the Fourth Amendment required courts to regulate "camera surveillance of public activity."[261] This argument was an open rebuke to *Knotts*' allowance of using radio beepers to track vehicle movement in public spaces. *Knotts* acknowledged the concerns that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision." Therefore, "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[262] Slobogin believed the conditions of urban life in the Post 9/11 world described the situation hypothesized in *Knotts*. Slobogin based his argument on the duty of the Court to protect the public's reasonable expectation of privacy. There was no discussion as to whether the Court was the proper institution to be the defender of citizens' right to privacy. "Public Privacy" asserted "'a right to anonymity,' even when in public" based on the Freedom of Expression.[263] One's behavior is an expression of our private thoughts; because First Amendment rights

[260] Christopher Slobogin, "An Original Take on Originalism," Responding to Orin Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harvard Law Review 476 (2011); Orin Kerr, "Defending Equilibrium-Adjustment," Responding to Christopher Slobogin, "An Original Take on Originalism," 125 Harvard Law Review 14 (2011).
[261] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," 72 Mississippi Law Journal 213-315 (2002) (symposium), 215.
[262] *United States v. Knotts*, 460 U.S. 276, 283-284 (1984).
[263] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," 72 Mississippi Law Journal 213-315 (2002) (symposium), 216.

protect our words, our innocuous conduct should also be protected by the Fourth Amendment. Slobogin's arguments were supported by political theory, legal scholarship, and quantitative social psychology. The suggested remedy to reduce the harm caused by widespread surveillance was "minimal guidelines" and "monitoring police decisions" to ensure reasonable conduct.

In "Government Dragnets," Slobogin argued that Programmatic Searches in the digital era failed to meet the "reasonableness" standard of the Fourth Amendment.[264] Slobogin defined a government dragnet as,

> programmatic government efforts to investigate, detect, deter, or prevent crime or other significant harm by subjecting a group of people, most of whom are concededly innocent of wrongdoing or of plans to engage in it, to a deprivation of liberty or other significant intrusion.[265]

Slobogin criticized the Court's progressive leniency of the post-Warren Court towards Programmatic Searches and "special needs" searches. Slobogin wanted the Court to return to the Warren-era jurisprudence of *Camara* and *See*, which ruled that nonconsensual administrative searches of residential and commercial properties were not immune from probable cause and warrant requirements absent emergency conditions.[266] *Camara* and *See* did not remain intact for long. In *Colonnade v. United States* and *United States v. Biswell*, not five years after *Camara*, the Court permitted warrantless non-forced entry by federal inspectors of a liquor store and gun store.[267] The Court then saw fit to permit Immigration and Driving Under the Influence (DUI) roadblocks,[268] so long as the purpose of the search was not detection

---

[264]Christopher Slobogin, "Government Dragnets," 73 Law and Contemporary Problems 107, Summer 2010, 108-109, https://scholarship.law.vanderbilt.edu/faculty-publications/250, accessed December 10, 2021

[265]Christopher Slobogin, "Government Dragnets," 73 Law and Contemporary Problems 107, Summer 2010, 110.

[266] *Camara v. Municipal Court*, 387 U.S. 523 (1967), *See v. City of Seattle*, 387 U.S. 541 (1966)

[267] Colonnade Catering Corp. v. United States, 397 U.S. 72 (1970), United States v. Biswell, 406 U.S. 311 (1972)

[268] *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), *Michigan Department of State Police v. Sitz*, 496 U.S. 444 (1990)

of “ordinary criminal wrongdoing.”[269] Next, the Court softened mandatory warrantless drug testing and searches of government employees and public school students.[270] Across the business inspections, roadblocks, and drug testing, Slobogin argued that the Court approved “almost any colorable demonstration of government need.”[271] Slobogin then cautioned against public camera surveillance systems and data mining for law enforcement purposes, regardless of success rates. This led to a harsh critique against the Court’s position on the Third Party and Public View doctrines which permit such forms of data compiling, analysis, and exploitation. Slobogin summarized the jurisprudence towards dragnets to pertain to one or more of the following factors: Is the situation special needs? How significant is the government's interest? How significant is the problem? Would an individualized-suspicion requirement prevent the government from achieving its goal? How intrusive is the dragnet? Is the dragnet noticeable or intrusive? What level of review will the dragnet require? Are there neutral means to narrowly apply the dragnet?[272] As a result, only the most irrational dragnets have been rejected by the Court. Slobogin was not satisfied with the status quo and suggested a proportionality principle derived from *Camara* that “the justification required for a search program—defined in terms of the likelihood that the search or seizure will obtain evidence of wrongdoing—should be roughly proportionate to its intrusiveness.”[273] This approach both accounts for exigent searches and honors the “expectations of privacy society is prepared to recognize as reasonable,” the second part of Harlan’s establishment of the “reasonable expectation of privacy.” The application of the proportionality principle in investigations would require that “the intrusiveness of a government

[269] *Indianapolis v. Edmond*, 531 U.S. 37 (2000)
[270] *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), *Skinner v. Railway Lab. Execs. Ass'n*, 489 U.S. 602 (1989), *Nat'l Treas. Emp. Union v. Von Raab*, 489 U.S. 656 (1989), *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995), *Chandler v. Miller*, 520 U.S. 305 (1997)
[271] Christopher Slobogin, “Government Dragnets,” 73 Law and Contemporary Problems 107, Summer 2010, 120, https://scholarship.law.vanderbilt.edu/faculty-publications/250, accessed December 10, 2021
[272]Christopher Slobogin, “Government Dragnets,” 73 Law and Contemporary Problems 107, Summer 2010, 127, https://scholarship.law.vanderbilt.edu/faculty-publications/250, accessed December 10, 2021
[273]Christopher Slobogin, “Government Dragnets,” 73 Law and Contemporary Problems 107, Summer 2010, 138, https://scholarship.law.vanderbilt.edu/faculty-publications/250, accessed December 10, 2021

action dictates the justification necessary to carry it out."[274] The purpose is to require *ex-ante* review for anything outside of exigent circumstances.[275]

In "Is the Fourth Amendment Relevant in a Technological Age?"[276] Slobogin expanded concerns from "Government Dragnets" and applied them to developing technologies. Slobogin described a slightly futuristic picture that began with a justifiable traffic stop and quickly turned into a total dragnet on an unsuspecting individual, including a warrantless GPS device, persistent surveillance from pole cameras, license plate readers, drones, digital records from the individual's internet service provider, bank, and credit cards, topped off with a surveillance unit across the street with low-light capabilities. Aside from the GPS device, the other records can be acquired with a subpoena or no additional barriers due to the legal doctrines previously discussed. Slobogin believed these to be a serious threat to the average person. He developed the proportionality principle to recommend further a reformed understanding of "search" to include "Camera surveillance, tracking, targeting places or people with devices (whether or not they are in general public use or contraband-specific), and accessing records via computer all involve searches under this definition."[277] Therefore, searches for civil litigation would have a lower standard than criminal investigations.

> A more formal adoption of the proportionality principle would state that, for every government action that implicates the Fourth Amendment, government must demonstrate "cause"—defined as the level of certainty that evidence of wrongdoing will be found—roughly proportionate to the intrusiveness of the search.[278]

---

[274]Christopher Slobogin, "Government Dragnets," 73 Law and Contemporary Problems 107, Summer 2010, 139, https://scholarship.law.vanderbilt.edu/faculty-publications/250, accessed December 10, 2021
[275]Christopher Slobogin, "Government Dragnets," 73 Law and Contemporary Problems 107, Summer 2010, 141, https://scholarship.law.vanderbilt.edu/faculty-publications/250, accessed December 10, 2021
[276] Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?* in *The Future of The Constitution* 11-36 (Jeffrey Rosen & Benjamin Wittes, eds.) (Brookings Institute, 2012) (abbreviated version in The Constitution and the Future of Criminal Justice in America (John Parry & Song Richardson, eds., Cambridge Univ. Press, 2012), accessed November 8, 2021 https://www.brookings.edu/research/is-the-fourth-amendment-relevant-in-a-technological-age/
[277] Christopher, Slobogin, *Is the Fourth Amendment Relevant in a Technological Age? in The Future of The Constitution*, 11-36 (Jeffrey Rosen & Benjamin Wittes, eds.) (Brookings Institute, 2012) 14.
[278] Christopher, Slobogin, *Is the Fourth Amendment Relevant in a Technological Age? in The Future of The Constitution*, 11-36 (Jeffrey Rosen & Benjamin Wittes, eds.) (Brookings Institute, 2012) 15.

Slobogin also proposed a reform to group searches. With the proportional approach applied, "individual suspicion" would be replaced with "generalized suspicion"; thus, the search may be justified depending on the accuracy to which a particular group is programmatically searched. Slobogin argued for these reforms because he did not believe a sufficient right to privacy exists in public spaces.[279]

Thus far, Slobogin would consider WAPS to be a dragnet in persistent violation of one's right to free expression. The proportionality principle was an adaptation of a Mosaic Theory because it considered the totality of events as the primary means of justification. It rejected the sequential approach which Kerr relies upon and supports. It is also important to recognize how the "special needs" or Programmatic Search doctrine might come into play when evaluating WAPS systems. It would not be out of character for a court to determine WAPS as a search. However, because of the conditions of operations, such as prohibitions against analysis without a probable cause first being established, one would find the invasive qualities of WAPS against the general public sufficiently incidental to be permissible as a Programmatic Search. Slobogin's approach to Programmatic Search, Third Party, and Public View doctrines call for a paradigm shift to Fourth Amendment jurisprudence that would go further than embracing a Mosaic Theory.

Slobogin rejected Kerr's Equilibrium Adjustment theory due to what he believed was its inherently Originalist approach, which he also rejected.[280] Slobogin also pointed to the non-originalist origins of the Common Use rule from *Kyllo*, the Third Party doctrine from *Smith*, and numerous conditions under the "special needs" doctrine in the post-*Katz* jurisprudence of the

[279] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," 72 Mississippi Law Journal 213-315 (2002) (symposium).
[280] Christopher Slobogin, "An Original Take on Originalism," Responding to Orin Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harvard Law Review 476 (2011) https://harvardlawreview.org/2012/01/an-original-take-on-originalism/ accessed Dec 2, 2021.

Fourth Amendment.[281] His primary critiques targeted Kerr's "Year Zero" which Slobogin believed was in the 18th century. Kerr responded to Slobogin's arguments arguing that Equilibrium Adjustment theory is not based on Originalism but rather on maintaining the status quo in Fourth Amendment jurisprudence.[282]

In "Making the Most of *United States v. Jones* in a Surveillance Society," Slobogin hoped to provide a statutory framework to apply the Mosaic Theory as described by the Alito and Sotomayor concurrences.[283] However, the Court has not explicitly embraced either Mosaic Theory in its more recent cases. In the article, Slobogin linked the protections against searches and seizures in the same way the entire Bill of Rights protects liberty and dignity by restricting government power. Slobogin arguably has the most expansive reading of "unreasonable searches and seizures," saying, "I have taken the position that any government effort to observe or find out about a person's activities, transactions, or communications is a Fourth Amendment search."[284] If the most incidental contact or inquiry is an unreasonable search or seizure, one would be hard-pressed to preserve any investigatory powers that might survive without prior probable cause. The article is primarily a statutory suggestion and explainer to concretely establish a legislative proportionality principle described in "Government Dragnets."

In "Policing, Databases, and Surveillance," Slobogin critiqued five categories of government databases containing personal information: "suspect-driven; profile-driven; event-

[281] *Kyllo v. United States*, 533 U.S. 27 (2001), *Smith v. Maryland*, 442 U.S. 735 (1979); An Original Take on Originalism by Christopher Slobogin, Responding to Orin Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harvard Law Review 476 (2011), 19.
[282] Kerr, Defending Equilibrium-Adjustment: Responding to Christopher Slobogin, *An Original Take on Originalism*, 125 Harvard Law Review 14 (2011), 86-7.
[283] Christopher Slobogin, "Making the Most of *United States v. Jones* in a Surveillance Society: A Statutory Implementation of Mosaic Theory," 8 Duke Journal of Constitutional Law & Public Policy 1-37 (2012) accessed June 29, 2021, https://scholarship.law.duke.edu/djclpp/vol8/iss1/1
[284] Christopher Slobogin, "Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory," 8 Duke Journal of Constitutional Law & Public Policy 1-37 (2012) accessed June 29, 2021, https://scholarship.law.duke.edu/djclpp/vol8/iss1/1

driven; program-driven and volunteer-driven."[285] The databases at issue include "Google, Netflix, and Apple; the memory banks of phones, closed-circuit cameras, "smart cars," and satellites; and the computers in government agencies and commercial establishments."[286] The concern is to identify "when the government should be able to gain access to this wealth of personal information for law enforcement and national-security purposes."[287] This approach recognized that the kind of personal information revealed from such databases did not rise to the level of probable cause/warrant requirements but could still significantly hinder government interests in enforcing crime and preventing terrorism. Before giving law enforcement access to the databases, the proposed criterion should be applied. It was a thoughtful recognition of both the digital realm's role in the present life and what now constitutes an "unreasonable search or seizure." It was a strong reminder of the Fourth Amendment's inherently subjective standard of "unreasonable."

The proportionality principle was discussed more thoroughly in "Policing as Administration."[288] The bulk of the article proposed applying the administrative rule-making procedure to law enforcement agencies. It also articulated the differences between suspicionless searches without individualized suspicion versus those with suspicion. Government actions without individualized suspicion were mere data collection. The proportionality principle and Fourth Amendment concerns were not triggered until an

[285] Christopher Slobogin, "Policing, Databases and Surveillance: Five Regulatory Categories," (April 6, 2017), National Constitution White Paper Series (2017, Forthcoming), Academy for Justice: A Report on Scholarship and Criminal Justice (Erik Luna ed., 2017, Forthcoming) , Vanderbilt Law Research Paper No. 17-23, 70, https://ssrn.com/abstract=2947948

[286] Christopher Slobogin, "Policing, Databases and Surveillance: Five Regulatory Categories," (April 6, 2017), National Constitution White Paper Series (2017, Forthcoming), Academy for Justice: A Report on Scholarship and Criminal Justice (Erik Luna ed., 2017, Forthcoming) , Vanderbilt Law Research Paper No. 17-23, 71, https://ssrn.com/abstract=2947948

[287] Slobogin, Christopher, "Policing, Databases and Surveillance: Five Regulatory Categories (April 6, 2017)," National Constitution White Paper Series (2017, Forthcoming), Academy for Justice: A Report on Scholarship and Criminal Justice (Erik Luna ed., 2017, Forthcoming), Vanderbilt Law Research Paper No. 17-23, 71, https://ssrn.com/abstract=2947948

[288] Christopher Slobogin, "Policing as Administration," 165 University of Pennsylvania Law Review 91 (2016), accessed May 18, 2022, https://scholarship.law.upenn.edu/penn_law_review/vol165/iss1/3

individualized suspicion, including an event or person of interest, was identified. Once there was a person or event to be focused on, the proportionality principles should be applied. They would likely succeed because the potential level of intrusion was more narrowly focused. In "Suspectless Searches," Slobogin applied the principles from "Policing, Databases, and Surveillance" to geofencing, "TiVo Droning " which is WAPS, DNA matching, Automated License Plate Readers, and facial recognition technology.[289] Because WAPS operates without individualized suspicion as it collects the imagery, as long as the analysis (or TiVoing) of the data follows after probable cause is established, WAPS is constitutional, according to Slobogin's analysis.[290] To that effect, the proportionality principle was workable for scholars and law enforcement conducting investigations, whether it be bulk or consolidated across numerous collection points. Given Slobogin's prior analyses, finding any model in which WAPS would be permissible was surprising. At the same time, "Policing, Databases, and Surveillance" analyzed each technology in sequential isolation, the same model of analysis Kerr advocated. Slobogin likely would not support the TiVo droning was it combined with other surveillance networks as it was in Baltimore's AIR program.

David Gray and Danielle Citron co-authored four articles in 2013 addressing the collisions between new technologies and the Fourth Amendment. The benefit the Mosaic Theory presented was a framework that, in their view, could more adequately address mass data aggregation and surveillance. The primary doctrinal challenge the Mosaic Theory presented was the abandonment of Public View and Third Party doctrines.[291] Their practical

[289] Christopher Slobogin, "Suspectless Searches," Vanderbilt Law Research Paper No. 21-38, 7-8, September 3, 2021, accessed April 30, 2022, https://ssrn.com/abstract=3917150 or http://dx.doi.org/10.2139/ssrn.3917150

[290] Christopher Slobogin, "Suspectless Searches," Vanderbilt Law Research Paper No. 21-38, 8, September 3, 2021, accessed April 30, 2022, https://ssrn.com/abstract=3917150 or http://dx.doi.org/10.2139/ssrn.3917150

[291] David Gray & Danielle K. Citron, "A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy," 14 North Carolina Journal of Law & Technology 381 (2013), 401-405, accessed July 9, 2021, http://scholarship.law.unc.edu/ncjolt/vol14/iss2/3

criticism of the Mosaic Theory was the difficulty of drawing lines between acceptable data aggregations and violations.[292] The Mosaic Theory focused on "how much" data was too much. Gray and Citron focused on "how" data were collected.[293] The same criticism of Kerr. The line-drawing problems of the Mosaic Theory were not isolated. The subjective nature of the "reasonableness" standard is inherent to the Fourth Amendment. In response to the shortcomings of the mosaic theory [sic], they proposed the right of Quantitative Privacy.[294]

> Quantitative Privacy was concerned with how information was collected, whether an investigative technique or technology has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government.[295]

The test Gray and Citron suggested was based on three factors, "(1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs associated with deploying and using the technology."[296] Quantitative Privacy was the result of the Information Privacy Law Project, a cohort of "scholars, activists, and policymakers working on information privacy law have warned about the dangers of surveillance technologies."[297] Quantitative Privacy did not necessarily provide a clear, quantifiable measure to apply to its Fourth Amendment challenges. Though a model similar to

---

[292] David Gray & Danielle K. Citron, "A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy," 14 North Carolina Journal of Law & Technology 381 (2013), 408, accessed July 9, 2021, http://scholarship.law.unc.edu/ncjolt/vol14/iss2/3

[293] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, U of Maryland Legal Studies Research Paper, 2013-23, 71, accessed May 14, 2021, https://ssrn.com/abstract=2228919

[294] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, U of Maryland Legal Studies Research Paper, 2013-23, 71-72, https://ssrn.com/abstract=2228919

[295] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, U of Maryland Legal Studies Research Paper, 2013-23, 101, https://ssrn.com/abstract=2228919

[296] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, U of Maryland Legal Studies Research Paper, 2013-23, 102, https://ssrn.com/abstract=2228919

[297] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, U of Maryland Legal Studies Research Paper, 2013-23, 69, https://ssrn.com/abstract=2228919

PUBLIC SURVEILLANCE

1. Looking in foliage in park	8 +/-4
2. Conducting health and safety inspection of factory	14 +/-4
3. Monitoring cameras at national monuments	20 +/-7
4. Monitoring cameras at government buildings, airports, train stations	20 +/-7
5. Inspecting a coal mine	25 +/-5
6. Monitoring cameras at stores	26 +/-8
7. Stopping drivers at roadblock for fifteen seconds	35 +/-5
8. Monitoring covert street cameras that have zoom capacity	42 +/-9
9. Flying helicopter 400 feet over backyard	50 +/-5
10. Conspicuously following person down street	50 +/-5
11. Going through garbage cans at curbside	51 +/-5
12. Searching a junkyard	51 +/-5
13. Monitoring overt street cameras; tapes destroyed after ninety-six hours	53 +/-8
14. Monitoring a beeper on a car for three days	63 +/-5
15. Using a device that can see through clothing to detect outline of items	67 +/-5
16. Conducting a pat down of outer clothing; feeling for weapons	68 +/-5
17. Using a video camera to overhear a conversation on the street	70 +/-5
18. Same as 13 above, but tapes not destroyed	73 +/-8
19. Searching body cavities at border	75 +/-5
20. Searching a bedroom	76 +/-5

Slobogin's Public Surveillance chart from *Privacy at Risk* might be useful. In the chart, Slobogin scored different activities according to their "intrusiveness" such that if a collection of investigative activities surpasses a particular value, the activities would be unconstitutional.[298] Gray and Citron, like Slobogin, were concerned with data aggregation and surveillance technologies, which in their view, unnecessarily collect information about people outside the scope of law enforcement investigations. Quantitative Privacy was novel and has not been adopted in any prominent Fourth Amendment cases.[299]

[298] Orin Kerr, "Do We Need a New Fourth Amendment?," 107 Michigan Law Review 561 (2009), 954, https://ssrn.com/abstract=1236522

[299] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, U of Maryland Legal Studies Research Paper, 2013-23, 92, https://ssrn.com/abstract=2228919

Since the publication of Quantitative Privacy, Citron has focused further research on sexual privacy.[300] Gray has continued to develop Quantitative Privacy. Gray described the approaches to the Mosaic Theory as durational, content-based, or technology-centered. Justice Alito's *Jones* concurrence was classified as a durational approach. Gray was concerned that the durational approach did not provide an adequate framework to maintain human surveillance techniques, which rest on decades of Fourth Amendment jurisprudence.[301] Gray believed Slobogin's proportionality principle was a good innovation to the durational approach, but to implement it would still require significant changes to the Third Party and Public View doctrines.

The content-based approach was a creation by First Amendment scholar Neil Richards. By merging it with Surveillance Studies, Richards challenged surveillance practices on the First Amendment's freedom of association grounds. The understanding is that surveillance (power) hierarchies exist between the surveilled and the surveyor.[302] Surveillance Studies, as a field, is a branch of Critical Studies scholarship with a focus on power hierarchies and the deconstruction of existing institutions and practices due to their purposeful, designed systemic oppression. Arguments from the Surveillance Studies scholarship have been cited in federal court opinions, such as *Leaders of a Beautiful Struggle*. However, the Supreme Court has not endorsed its framework in any Fourth Amendment jurisprudence.

The durational and content-based approaches both violate the core principle of constitutional neutrality.[303] According to Gray, the technology-centered approach was less

---

[300] Danielle Keats Citron, University of Virginia School of Law Faculty Profile, accessed June 1, 2022, https://www.law.virginia.edu/faculty/profile/ugg7tt/2964150

[301] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, accessed February 26, 2021, https://digitalcommons.law.umaryland.edu/books/111, 117-118.

[302] Neil Richards, "The Dangers of Surveillance," 26 Harvard Law Review 1934, 2013, accessed May 3, 2022, https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/, (Richards did not coin the phrase content-based)

[303] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, 117-118, accessed February 26, 2021, https://digitalcommons.law.umaryland.edu/books/111, 123

disruptive to existing law enforcement practices, particularly human surveillance practices. Gray found human surveillance as a preferable form of surveillance to preserve because unlike technology-based surveillance, it cannot be practically scaled in the same way technology-based surveillance is. The scaling surveillance was also one of Justice Alito's arguments in his Jones concurrence.[304] Gray argued that the Court applied a technology-centered approach in *Riley v. California*.[305] By the court extending protection to a cellular phone in the same way it had done to a bag, wallet, or desk drawer, the decision was because "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—unless the phone is."[306] Even though the technology-centered approach was the best approach, according to Gray, it was still insufficient because,

> There are as of yet no "different constitutional principles" that would allow threats of broad and indiscriminate surveillance posed by "dragnet type law enforcement practices" to trigger Fourth Amendment concerns much less underwrite rules that would limit access to these kinds of means and methods.[307]

Hence, Gray shifts focus toward a collective right to privacy.

Gray believed the original public meaning of the Fourth Amendment, in an analytical approach Justice Alito would approve of, should be understood as a collective right in addition to an individual right.[308] Interestingly enough, this analysis also aligned with Justice Breyer's "active liberty" approach to the Constitution.[309] Between the corporate language of "the people"

---

[304] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, 117-118, accessed February 26, 2021, https://digitalcommons.law.umaryland.edu/books/111, 127.
[305] *Riley v. California*, 573 U.S. 373 (2014), in this case the Court ruled law enforcement cannot search the contents of a cellular phone without a warrant, even if the phone is on a person incident to an arrest.
[306] *Riley v. California*, 573 U.S. 397 (2014)
[307] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, 117-118, accessed February 26, 2021, https://digitalcommons.law.umaryland.edu/books/111, 128.
[308] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, 117-118, accessed February 26, 2021, https://digitalcommons.law.umaryland.edu/books/111, 134-189.
[309] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, https://digitalcommons.law.umaryland.edu/books/111, 155, citing Stephen Breyer,

and well-documented concern of general warrants at the time of the Founding, Gray argued that the Fourth Amendment was designed to protect the collective rights against unreasonable searches and seizures as a matter of the text. According to the collective right to privacy, the Public View and Third Party doctrine was incompatible. The collective right to privacy further abandoned *Katz* and all its exceptions to what was constitutionally considered "searches" for a more original public meaning of "search." Such an expansion of the scope of the definition of "search" would overturn the majority of the Court's Fourth Amendment jurisprudence of the last five decades.[310] Gray has continued to develop the collective right to privacy by challenging current search and seizure practices such as Stop and Frisk,[311] Big Data,[312] and facial recognition.[313]

The earliest legal publications on WAPS were published in 2018 as law Notes.[314] John Pavletic and Andrea Carlson wrote each Note following the Reel's Bloomberg article but added circuit and Supreme Court precedents analysis.[315] Pavletic analyzed the use of WAPS described in the article as a hypothetical federal case. Pavletic argued that WAPS should be considered in the same way as the Court addressed GPS tracking. However, because there was no trespass by the aerial surveillance, Judge Ginsberg's Mosaic Theory should analyze

---

Active Liberty: Interpreting Our Democratic Constitution, New York: Knopf Doubleday Publishing Group (2006).

[310] David Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press, 2017, 111, https://digitalcommons.law.umaryland.edu/books/111, 134-249.

[311] David Gray, "Collective Standing under the Fourth Amendment," Georgetown Law (American Criminal Law Review, 2018), https://www.law.georgetown.edu/american-criminal-law-review/in-print/volume-55-issue-1-winter-2018/collective-standing-under-the-fourth-amendment/.

[312] David Gray, "Collective Rights and the Fourth Amendment After Carpenter," 79 Maryland Law Review 66 (2019), https://digitalcommons.law.umaryland.edu/mlr/vol79/iss1/4

[313] David Gray, "Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies," 24 Southern Methodist University Science & Technology Law Review 3 (2021) https://scholar.smu.edu/scitech/vol24/iss1/2

[314] "Types of Notes," Types of Notes (NYU School of Law), accessed June 9, 2022, https://www.law.nyu.edu/students/studentwriting/typesofnotes.

[315] John Pavletic, "The Fourth Amendment in the Age of Persistent Aerial Surveillance," 108 Criminal Law & Criminology 171 (2018). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4; Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 167-196.

WAPS. Pavletic relied on *United States v. Cuevas-Sanchez*, a Fifth Circuit case that ruled against a pole camera to counter *Ciraolo*'s Flyover precedent.[316] Additionally, the Fourth Circuit's ruling on what would later become *Carpenter* ruled CSLI data to be a search via the Mosaic Theory. However, the Supreme Court reversed and remanded the Fourth Circuit's ruling, denying the Mosaic Theory constitutional legitimacy.[317] Pavletic concluded WAPS to be an unconstitutional search.

Carlson conducted a more thorough constitutional analysis focusing on the Flyover Cases, *Kyllo*, *Jones*, and *Katz*. Carlson did not embrace a Mosaic Theory because "neither the majority nor concurrences wholeheartedly adopted the Mosaic Theory."[318] Without embracing a Mosaic Theory, Carlson acknowledged the difficulty in restricting WAPS. For example, if the Court sought to apply a trespass to an aerial platform, they would have to revisit *Causby*.[319] In *Causby*, a chicken farmer claimed a property loss because government jet-powered aircraft flew "83 feet above his property," leading to the subsequent panic and death of numerous chickens and the farm's closing. The Court acknowledged a degree of airspace the property owner has "at least as much of the space above the ground as he can occupy or use in connection with the land."[320] Based on *Florida v. Riley*, the upper limit a property owner may be able to claim successfully is 400 feet above ground level (AGL).[321] Carlson relied on Kerr's criticisms of the Mosaic Theory to recommend legislative responses to WAPS.[322]

---

316 *United States v. Cuevas-Sanchez* 821 F.2d 248, 251 (5th Cir. 1987), *California v. Ciraolo*, 476 U.S. 207 (1986)
317 *United States v. Graham*, 824 F.3d 421, 447–48 (4th Cir. 2016).
318 Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 184.
319 *United States. v. Causby*, 328 U.S. 256 (1946).
320 Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 185.
321 *Florida v. Riley*, 488 U.S. 445, 451 (1989)
322 Andrea Carlson, "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment," University of Illinois Journal of Law, Technology & Policy 2018, no. 1 (Spring 2018): 188-194.

Andrew Ferguson of American University Washington College of Law has done the most direct and thorough legal analysis of WAPS to date.[323] In the forthcoming article "Persistent Surveillance," Ferguson homed in on "persistent surveillance" from a stationary pole camera and WAPS from *LBS* and *United States v. Tuggle*, a case the Supreme Court denied cert in February 2022.[324] In *Tuggle*, law enforcement placed three fixed wide-angle cameras on poles around his property in public spaces for eighteen months without a warrant. The Seventh Circuit relied on the Flyover Cases and upheld the use of pole cameras.[325] Neither Kerr, Gray, nor Citron has published specific analyses on persistent surveillance or WAPS. Slobogin's attention to WAPS in "Suspectless Searches" was brief.[326] Like the other legal scholars, Ferguson identified what were believed to be insufficient existing models of analysis of this new technology and provided a new framework for them.

The long-term goal was to provide a framework for "all future persistent surveillance technologies used by police without a warrant."[327] Ferguson argued that the scale, duration, and reach separated persistent surveillance from traditional forms of surveillance.[328] Once a court recognized the concerns of persistent surveillance, Ferguson suggested a seven-part test, primarily based on *Jones*, *Riley v. California*, & *Carpenter*.[329] Ferguson defined the question as a matter of what is the "unit of surveillance?" Is it based on the capacity for collection or the

---

[323] Andrew Guthrie Ferguson, "Persistent Surveillance" (March 31, 2022). Alabama Law Review, Forthcoming, https://ssrn.com/abstract=4071189

[324] *United States v. Tuggle*, 4 F.4th 505, 2021 U.S. App. LEXIS 20841, 2021 WL 2946100 (United States Court of Appeals for the Seventh Circuit July 14, 2021, Decided). https://advance-lexis-com.ccl.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:634S-BWJ1-JKPJ-G3P5-00000-00&context=1516831.

[325] *United States v. Tuggle*, 4 F.4th 505, 513, 2021 U.S. App. LEXIS 20841, *11, 2021 WL 2946100 (7th Cir. Ill. July 14, 2021)

[326] Slobogin, Christopher, "Suspectless Searches," Vanderbilt Law Research Paper No. 21-38, (September 3, 2021), accessed April 30, 2022, https://ssrn.com/abstract=3917150, 7-8.

[327] Andrew Guthrie Ferguson, "Persistent Surveillance" (March 31, 2022), Alabama Law Review, Forthcoming, 4, https://ssrn.com/abstract=4071189

[328] Andrew Guthrie Ferguson, "Persistent Surveillance" (March 31, 2022), Alabama Law Review, Forthcoming, 3, https://ssrn.com/abstract=4071189

[329] Because *Florida v. Riley* (1989) and *Riley v. California* (2014) can and are often both referred to as "Riley," the full case name will be used to avoid confusion.

actual collection in a specific case?[330] To answer this question, the technology in question should be identified as either a "tool" or a "system." The more the technology is a system, the greater the level of scrutiny to be applied. The tool or system model can be adequately demonstrated in *Kyllo*, *Jones*, *Riley v. California*, and *Carpenter*. It also assisted in differentiating if a case was concerned with an isolated data point or if it was part of a more extensive network of assets. The concern over the capacity of the technology or the use of the technology in specific cases remains unanswered. Ferguson then analyzed *LBS* and *Tuggle* under the provided criteria. *LBS* was certainly a system because it integrated WAPS with other networks of surveillance technologies such as CitiWatch, Shotspotter, and Automated License Plate Readers (ALPR).[331] Thus the en banc opinion in *LBS* was not based only on WAPS but the totality of the AIR Pilot Program encompassing multiple technologies. Likewise, although the Seventh Circuit court in *Tuggle* viewed the three pole cameras as stand alone tools, Ferguson argued the "vast stores of digital information… stored data that went back to FBI headquarters" merged with "other investigative resources" which may include "license plates, photos for identification, and other clues" constituted a system. "There is a world of difference between police using a camera to watch your front door, and a police officer being able to access a saved searchable database of images from your front door for the past 18 months connected to other police datasets of personal information."[332] Ultimately, Ferguson's concerns were centered around the aggregated data factor, which was the heart of the Mosaic Theory. Ferguson's approach was a distinct form but still a form in kind.

The bulk of scholarship concerning WAPS and the Fourth Amendment is unclear. Either one applies a sequential approach, under which neither the courts nor legislatures have

[330] Andrew Guthrie Ferguson, "Persistent Surveillance" (March 31, 2022), Alabama Law Review, Forthcoming, 35, https://ssrn.com/abstract=4071189
[331] Andrew Guthrie Ferguson, "Persistent Surveillance" (March 31, 2022), Alabama Law Review, Forthcoming, 44, https://ssrn.com/abstract=4071189
[332] Andrew Guthrie Ferguson, "Persistent Surveillance" (March 31, 2022), Alabama Law Review, Forthcoming, 47-48, https://ssrn.com/abstract=4071189

adjusted any of the equilibriums prompted by this new technology, or a Mosaic Theory focused on the aggregated data and analysis process, which would initiate a paradigm shift in Fourth Amendment interpretation and application. WAPS is constitutional if the Fourth Amendment is to be maintained along the "Equilibrium-Adjustment" model, which is an approximate status quo for the new technologies. If a novel approach like a Mosaic Theory, qualitative approach to the Fourth Amendment, proportionality principle, collective right to privacy, or the seven A's are to be adopted, it is not.[333]

Justification of the Problem

WAPS is among the least intrusive new surveillance technologies developed in the digital age compared to facial recognition, CSLI, GPS, Smartphone applications, ALPR, or Deep Mind predictive analysis. Its primary utility in a law enforcement capacity is the forensic capabilities, which require large amounts of warrantless imagery data collection. The Fourth Circuit evaluated WAPS for a Temporary Restraining Order (TRO) in *LBS*. The Federal District Court of Maryland denied the motion; the Fourth Circuit panel denied the motion, and the en banc panel granted the motion. However, the criteria for the TRO are distinct and specific to TROs. A constitutional analysis of the WAPS component of the AIR program has not been conducted by a federal court. The legal scholarship analyzing the constitutionality of WAPS based on the existing jurisprudence has not been published either. This dissertation does this task. As demonstrated in the literature review, there are several proposed frameworks to analyze surveillance technologies, which authors claim the Supreme Court has adopted. However, such adoptions have not yet been cited in any Supreme Court opinions. The Court denied the petition for certiorari for *Tuggle* in February 2022; *LBS* ended at the en banc panel of the Fourth Circuit Court of Appeals. The AIR Pilot Program's operations ceased in October

[333] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review, 2013, University of Maryland Legal Studies Research Paper, 2013-23, https://ssrn.com/abstract=2228919

2020. When the en banc panel granted the TRO in *LBS*, it sustained the use of archived data from the months the program was in operation. The constitutional fate of WAPS is unsettled law.

Because of the potential benefits of WAPS, it will likely be considered in many major cities across the United States in the coming years. This dissertation hopes to lay the analytical foundation for the legal considerations for city and state governments to consider when assessing if WAPS should be deployed. Unlike the current legal scholarship, this dissertation does not attempt to provide a new legal framework to interpret the Fourth Amendment's application to WAPS. It seeks to identify, under the present jurisprudence, the factors necessary to consider for WAPS to be used by state and local agencies. This is not the case for or against WAPS, but a detailed analysis of the factors, theories, and constitutional considerations which lawmakers and elected officials should weigh in policy deliberations as they govern their locales.

Chapter 4

WAPS is Constitutional

A plain text analysis of the most applicable cases does not prohibit WAPS deployment by state or city governments for law enforcement or any other purpose. The most applicable cases for this analysis are *Carpenter* and *Dow Chemical*. *Knotts* and *Karo*'s jurisprudence help the case for WAPS. Objections via *Kyllo* and *Jones* do not apply due to the limited types of information collected. The Open Fields doctrine does not apply outside of private property; even then, the limited information collected from viewing the open fields does not constitute a search. Under the second part of *Katz*'s reasonable expectation of privacy, the court has never held that law enforcement must have probable cause to view public spaces from the ground or air. Any objective constitutional concerns can quickly be addressed to comply with the Fourth Amendment's protections to the People. Because of the higher degrees of scrutiny the Fourth Amendment provides the People against law enforcement, much of this and the next chapter will address WAPS concerning the constitutionality of law enforcement's use of such

technology. The law enforcement deployment of WAPS would be the most likely state or local government use; the additional applications of WAPS would likely be seen as ancillary benefits but not primary over the public safety emphasis.

If WAPS were to be considered a search, it would be a "programmatic search" in which the public good it could provide outweighs the injury inflicted via *Martinez-Fuerte v. United States* (1976) and *Michigan Department of State Police v. Sitz* (1990).[334] *Martinez-Fuerte* challenged the incidental search of an interior Border Patrol checkpoint. The checkpoints were justified under the Federal Government's interest in enforcing immigration law and deterring illegal smuggling. All drivers along the designated highway were stopped for an incidental search at the checkpoint. During the search, the driver and vehicle occupants were briefly questioned before being permitted to continue on the highway. The incidental questioning would be used to possibly establish probable cause for a secondary search immediately after the initial inquiry. The Court held that "the stops and questioning at issue may be made in the absence of any individualized suspicion at reasonably located checkpoints."[335] The search, which was not identified as a Programmatic Search at the time, but would presently fit the definition today, on the degree of the compelled incidental interaction without any individualized suspicion. It is important to note that the Court was well aware of the significant negative hit rate of the checkpoints, where "only a small percentage of cars are referred to the secondary inspection area," indicating a degree of individualized suspicion.[336] *Sitz* was a case seeking injunctive relief against sobriety checkpoints operated by the Michigan State Police Department with the cooperation of the Saginaw County Sheriff's Department. *Sitz* argued probable cause and reasonable suspicion was absent in the sobriety checkpoint by checking all drivers along the

[334] *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976); *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, (1990)
[335] *United States v. Martinez-Fuerte*, 428 U.S. 543, 562 (1976)
[336] *United States v. Martinez-Fuerte*, 428 U.S. 543, 560 (1976)

given route. The Court weighed the liberty interest of the petitions against the state's interest in reducing drunk driving incidents.

> [W]here a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.[337]

Because the incidental stops lasted only 25 seconds,[338] the harm caused by such an incidental inconvenience was insufficient against the liberty rights claimed. *Sitz* was recognized as a Programmatic Search, which, like Martinez-Fuerte, lacked individual suspicion, but the state's compelling interest overruled the harm of stopping and incidentally questioning drivers. On these grounds, WAPS's ability to assist in any physical crime committed under the coverage area is clearly constitutional. The incidental harm from WAPS is objectively less than *Martinez-Fuerte* or *Sitz* because there are no personal interactions with law enforcement.

In *Dow Chemical*, the Court, in a 5-4 opinion, held that flying over private property for the purpose of surveillance with a high-resolution camera was not a violation of the Fourth Amendment.[339] The camera's resolution was high enough to capture items one-half inch in diameter. The EPA instigated the action to conduct regulatory inspections after being denied an on-site inspection for such inspections by Dow Chemical Company. In parts three and four, the Court ruled that the EPA was not limited to the methods prescribed by Congress to investigate and that the open-air site of the photographed area was akin to open fields.

The incorporation of the Fourth Amendment against the states via dicta in *Wolf v. Colorado* and formally in *Mapp v. Ohio* ensured the federal government and state governments were bound by the Constitution to protect the People's Fourth Amendment rights.[340] The Fourth Amendment is the controlling constitutional limitation because WAPS in any domestic capacity

---

[337] *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 449-450 (1990)
[338] *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 448 (1990)
[339] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986)
[340] *Wolf v. Colorado*, 338 U.S. 25 (1949) and *Mapp v. Ohio*, 367 U.S. 643 (1961)

of a populated area will surveil public and private property from various altitudes. It is important to note that the remedy for Fourth Amendment violations in *Mapp* is the application of the exclusionary rule. If WAPS is found to be an unreasonable search, the images collected would be legally rendered inadmissible. Although WAPS can benefit far more than law enforcement activities if cities are unable to use WAPS for law enforcement purposes, funding models without public safety interests would likely be prohibitive.

Fourth Amendment jurisprudence comparing regulatory searches versus criminal investigation searches is different; however, because regulatory searches maintain a lower burden of proof than probable cause warrant requirements, WAPS's constitutionality is not in danger. In 1967, *Camara v. Municipal Court of the City and County of San Francisco* ruled that Health Department Inspectors were required to obtain a warrant for inspections.[341] *Camara* overturned *Frank v. Maryland* which previously held that such inspections did not require a warrant.[342] Either way, because WAPS is aerial surveillance, wherein no government agents or officers step onto private property for a potential violation, these concerns do not apply to WAPS for law enforcement or regulatory inspections. Furthermore, Dow Chemical specifically protects such uses upon applying WAPS for regulatory enforcement. Upon application of WAPS for law enforcement purposes, other doctrines apply, namely, open fields and probable cause.

Dow Chemical did not address concerns over persistent surveillance; the EPA did not seek to maintain a watchful eye over the industrial site for regulatory enforcement.[343] However, *Knotts* and *Karo* inform the Court how the issue of persistent surveillance might be addressed.[344] *Carpenter* and *Jones* also apply.[345] I will demonstrate how WAPS does not become unreasonable searches under such precedents.

---

[341] *Camara v. Municipal Court*, 387 U.S. 523 (1967)
[342] *Frank v. Maryland*, 359 U.S. 360 (1959)
[343] *Dow Chemical Company v. United States*, 476 U.S. 227 (1986)
[344] *United States v. Knotts*, 460 U.S. 276 (1983) and *United States v. Karo*, 468 U.S. 705 (1984)
[345] *United States v. Jones*, 565 U.S. 400 (2012) and *Carpenter v. United States*, 585 U.S. 2206 (2018)

In *Knotts,* the Court ruled that the use of a radio transmitter placed by the cooperating seller in a barrel of chloroform for illicit purposes and the subsequent intermittent tracking of the radio signal and barrel over three days did not constitute an unreasonable search. In *Karo,* the Court similarly ruled that placing the tracking device, this time a 50-gallon barrel of ether, by a confidential informant who supplied the ether also did not constitute an unreasonable search or seizure. In both cases, devices were placed for intermittent visual surveillance for three (3) days and one hundred forty-three (143) days, respectively. In these cases, the intermittent periods of surveillance refer to waking hours and not 24-hour constant surveillance.

To remain constitutional, WAPS may need to refrain from collecting imagery 24 hours a day, seven days a week, without a warrant.[346] The contract at issue in Baltimore was for a minimum of forty hours per week but no more than twelve hours per day. No nighttime surveillance was permitted, analysts could not zoom in to any region without first report of specified felonies,[347] and the WAPS could not be used in a near-real-time capacity.[348] It may be that fiscal or efficiency purposes limit WAPS from operating at night. It may also be a Fourth Amendment compliance concern if 24-hour surveillance from a WAMI system were the proposed program. Therefore, the technological language of "persistent surveillance" and the legal language of "persistent surveillance" differ. Legally speaking, WAPS is only persistent if it is persistently operating. In *Knotts* and *Karo*, the facts did not provide explicit details to the degree the surveillance was maintained in a minute-by-minute or even hour-by-hour format. The *Karo* record does summarize months of surveillance. One would presume some degree of

[346] Such a warrant might only be issued under the most imminent emergencies.
[347] Shooting, Robbery, or Carjacking
[348] Talia Richman, "Baltimore Aerial Surveillance Agreement: $3.7 Million Price Tag, Privacy Protections, Evaluation Plan," *Baltimore Sun*, March 25, 2020, https://www.baltimoresun.com/politics/bs-md-pol-aerial-surveillance-agreement-boe-20200324-lvpjbsvqs5catntaeva2532a2a-story.html; Appeal Brief of Plaintiffs-Appellants in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, Case No. 20-1495, Fourth Circuit Court of Appeals, https://www.aclu.org/legal-document/appeal-brief-plaintiffs-appellants-0 accessed July 20, 2020.; Near-real-time capacity refers to using WAPS as a form of active overwatch during an operation, such as an active arrest or during the execution of a warrant.

persistent awareness was conducted to monitor the relocation of the barrel of ether successfully. In the same way, WAPS is always watching. If the data stream goes to a human analyst, they are not watching anyone or anywhere specifically unless there has been a cause to focus attention. The Department of Defense has long sought to use algorithmic software that could analyze persistent surveillance collection; however, such capabilities have not been publicized if it has been accomplished.[349] If or when such technology is developed and filtered to the state or local levels, the courts and legislatures must consider if such digital analysis must meet the probable cause standards of human investigators.

Knotts articulates the efficiency of using a radio transmitter versus maintaining manned surveillance. The technological advantage provided by the transmitter doing what would otherwise be done by an agent of the state was not a condition that affected the constitutionality of the persistent surveillance. The law enforcement agents were careful not to continue tracking the chloroform when it was moved to private property from public roads. This argument reappeared in *Carpenter*, where the court ruled against law enforcement for persistent tracking via the CSLI maintained and provided by the cellular service provider. *Knotts* and *Karo* should be more controlling on this specific point than *Carpenter*. In *Carpenter,* specific cellular phones belonging to the subjects of the investigation were exploited. In *Knotts* and *Karo*, the barrels of chemicals were the tracked items, not specific persons of interest. Likewise, with WAPS, although it is technically tracking everyone within its view, it is tracking no person in particular without an interest, presumably justified to zoom in on any specific person or area of interest. Even when a single person is surveilled, depending on the altitude or image-blurring software,

[349] Lance Menthe, Dahlia Anne Goldfeld, Abbie Tingstad, Sherrill Lingel, Edward Geist, Donald Brunk, Amanda Wicker, Sarah Lovell, Balys Gintautas, Anne Stickells, and Amado Cordova, "Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 2, Technical Analysis and Supporting Material," Santa Monica, CA: RAND Corporation, 2021, accessed February 1, 2023, https://www.rand.org/pubs/research_reports/RRA341-2.html, 45-63.

individuals are unlikely to be positively identified with WAPS. *Knotts* and *Karo* support using WAPS for law enforcement as long as specific individuals remain unidentified in the imagery.

The weakest challenge to the constitutionality of WAPS is a claim of general privacy from surveillance on public property. As previously mentioned, Open Fields and Plain View doctrines may apply; however, this is to clarify that such doctrines only potentially apply to private property. There are no reasonable expectations of privacy in public property or public access venues, particularly from aerial photographs. The Supreme Court first recognized the Open Fields doctrine in *Hester v. United States*.[350] The facts of *Hester* are brief and decisive. During Prohibition, federal revenue agents set up an observation area of the plaintiff's residence. They witnessed him hand a bottle to an associate. An officer pursued Hester, and in response, Hester dropped a glass jug and threw the bottle he was previously holding. The jug broke, but the expert analysis of the agents was able to accurately identify the remaining liquid in the jug as moonshine whiskey. Hester claimed the surveillance and arrest were illegal because the evidence seized was on his property without a warrant. The Court unanimously held that neither the observation nor the arrest violated Hester's rights. His actions witnessed by the officers were sufficient to prompt the arrest and collection of evidence.

> It is obvious that even if there had been a trespass, the above" testimony was not obtained by an illegal search or seizure. The defendant's own acts, and those of his associates, disclosed the jug; the jar and the bottle-and there was no seizure in the sense of the law when the officers examined the contents of each after it had been abandoned.[351]

The Court went further to cite Blackstone saying, "... the special protection accorded by the Fourth Amendment to the people in their "persons, houses, papers, and effects," is not extended to the open fields. The distinction between the latter and the house is as old as the common law."[352]

[350] *Hester v. United States*, 265 U.S. 57 (1924)
[351] *Hester v. United States*, 265 U.S. 57, 58 (1924)
[352] *Hester v. United States*, 265 U.S. 57, 59 (1924)

Hester was reaffirmed in *Oliver v. United States*, which presented similar facts to *Ciraolo* but at the ground level.[353] In *Oliver*, state law enforcement officers drove past a rural residence, ignoring the posted “no trespassing” signs to locate a plot of illicit substances growing on the property. The majority opinion rejected the claim that the illicit substances were “effects” covered under the Fourth Amendment. It highlighted the second part of the *Katz* test that “only those "expectation[s] that society is prepared to recognize as 'reasonable'" are protected. The Court noted that the mere signage was insufficient to demonstrate an expectation of privacy, further citing *Rakas*, stating, “No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant.”[354] This was also reaffirmed in *Ciraolo*, which argued that a taller fence also insufficiently demonstrated an expectation of privacy.[355] *Oliver* was significant by setting present-day common standards to the limits of Open Fields, “...we reaffirm today, may be understood as providing that an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.”[356]

Oliver's significant contribution to Fourth Amendment jurisprudence was the decisive rejection of the petitioner’s appeal to make a case-by-case approach to Fourth Amendment searches per *Katz*’s reasonable expectations of privacy. Citing *New York v. Belton,* the court replied, "'[a] highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions” would lead to an unworkable “ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances.”[357] Belton’s requirement alone might serve as the condemnation of the Mosaic Theory, as advocated by numerous Fourth Amendment scholars. However, the Court

[353] *Oliver v. United States*, 466 U.S. 170 (1984)
[354] *Rakas v. Illinois*, 439 U.S. 128 (1978)
[355] *California v. Ciraolo*, 476 U.S. 207, 211 (1986)
[356] *Oliver v. United States*, 466 U.S. 170, 178 (1984)
[357] *Oliver v. United States*, 466 U.S. 170, 181 (1984)

has not so much as mentioned it in either *Jones* or *Carpenter*, two opportunities in which it was most likely to appear if it were to curry acceptance. To be fair, Justice Sotomayor's concurrence in *Jones* did not use the term but certainly did present concern that a person may have from the government being able to track one's whereabouts. *Oliver* clarified and upheld the limitations of expectations of privacy that can only apply to private property and limited portions of the private property at that. To prohibit WAPS on a general right to privacy in public spaces would be akin to demanding patrol officers conduct patrol with their eyes closed until a call for assistance is made. This description of protected property versus unprotected property definitively establishes the inapplicability of a Fourth Amendment challenge to WAPS regardless of whether it collects imagery over Open Fields, shopping centers, or city plazas. In the same way, the Plain View doctrine is not controlling either because it exists as an exception to the search of a vehicle or private property based on what a law enforcement officer may view through the windows of the vehicle at issue. Plain View doctrine has evolved from Open Fields. Because Open Fields do not challenge WAPS, Plain View cannot be used to challenge it either.

The advanced nature of WAMI cameras does not make the government's use of them unconstitutional. The controlling case on this point is *Kyllo v. United States*.[358] In *Kyllo*, a federal agent suspected a marijuana grow house. Knowing that indoor marijuana grows require high-intensity lights late at night, from the street, he viewed the triplex with a thermal imager. The Court ruled against the use of the thermal imaging camera, " [when] the Government uses a device that is not in 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."[359] Here there is a two-part test concerning the use of new technology and the Fourth Amendment, 1) general public use and 2) obtaining the

[358] *Kyllo v. United States*, 533 U.S. 27 (2001)
[359] *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

information that would otherwise require physical intrusion. The General Public Use test was new.

The physical intrusion rule has been active since *Silverman v. United States*.[360] In *Silverman*, law enforcement officers pushed a spike microphone into a wall of an adjoining house to pierce into the heating duct of the room of interest. The duct was turned into an amplifier of which the officers listening to the recorded conversations testified incriminating evidence. The Court's unanimous opinion held that the microphone's physical intrusion was an unlawful trespass. The physical trespass or intrusion is the bright-line test to cross the Fourth Amendment. The majority opinion did not describe how to define when products were in "general public use." Justice Stevens' dissent cited the record of 5,000-6,000 units or similar units available for public use. He also noted "half a dozen national companies" readily available. Under Stevens' example, WAMI is not sufficiently proliferated to be considered for general public use; however, WAMI remains safe because it easily passes the second part of the test. This may ensure that night vision WAMI is not constitutional under the same grounds as Kyllo. However, night vision and thermal imaging devices in the last 19 years have likely proliferated sufficiently to be in "general public use." The Hawkeye II camera used by PSS in *LBS* is proprietary technology. However, PSS services are available to the public, and the infrared camera is not sensitive enough to reveal interior information from a structure. WAPS passes *Kyllo*.

Scholars have hypothesized how Unmanned Aerial Surveillance (UAS) systems, formerly called Unmanned Aerial Vehicles (UAV), can be challenged under *Kyllo*.[361] WAPS is not in danger. The current form of the platform is equipped on manned aircraft, which is extremely common under the "general public use" criteria. Potential challenges against the

[360] *Silverman v. United States*, 365 U.S. 505 (1961)
[361] Brandon Nagy, "Why They Can Watch You: Assessing the Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement," 29 Berkeley Technology Law Journal (2014), accessed April 15, 2021, https://ssrn.com/abstract=2429092

extensive range and detail of the WAPS cameras also fail to cause concern. The cameras employed in *LBS* have much less capacity for detail than the cameras and altitude used in *Dow Chemical*. The 4th Circuit paid significant attention to the fact that the AIR Program could not identify a person, nor could their "race, gender, or clothing" be identified. No positive identification would be possible via the AIR program without correlating ground-level surveillance assets, which under *Jones*, passed constitutional muster when the Court rejected the DC Circuit's embrace of the Mosaic Theory.

Unless the Court wants to identify a "unique nature"[362] of WAPS, it identified in *Carpenter* concerning CSLI; WAPS does not violate the Fourth Amendment. WAPS does not come close to the level of detailed personal information collected under *Carpenter*. In *Carpenter*, the Court held that warrants are only necessary for CSLI for more than six days. Even if WAPS in a particular jurisdiction was permitted to collect nighttime imagery, maintaining positive identification at night is impossible once the subject enters a building or vehicle with other occupants. The lack of continuous surveillance protects the constitutionality of the program. Even if the WAPS could identify an individual, their race, gender, or clothing, which could be possible if a smaller collection area were used by flying at a lower altitude or by using higher resolution cameras, it would still lack continuous coverage once the subject entered a structure or vehicle at night. Although the system includes "persistent surveillance" in its name, the legal precedent of its capacity is more accurately described as "intermittent."

Additionally, CSLI remains much more intrusive than WAPS, as it tracks subjects law enforcement is already monitoring. The two principal protections of WAPS against the Fourth Amendment are the intermittent nature and inability to identify subjects without other forms of surveillance or correlating assets. The accessibility of CSLI versus WAPS is also

[362] *Carpenter v. United States*, 138 U.S. 2217 (2018)

demonstratively significant. CSLI is much cheaper and more accessible for the state to collect, whereas WAPS requires detailed analysis from trained personnel.[363]

Even if WAPS were to be considered a search, the compelling state interest of the information collected for the public good would justify the degree of offense to the Fourth Amendment. It is unclear if WAPS could pass the strict scrutiny standard. It could most certainly meet intermediate scrutiny. The relevant cases are *United States v. Martinez-Fuerte* and *Michigan Department of State Police v. Sitz*. *Martinez-Fuerte* challenged the constitutionality of permanent border checkpoints within the United States along major highways away from the United States border. The Court acknowledged that vehicles were stopped absent any reasonable suspicion. The Court held "the government interests outweighed those of the private citizen" because the scrutiny one has from searches in a vehicle on a public highway does not offend "the sanctity of private dwellings, ordinarily afforded the most stringent Fourth Amendment protection."[364] The majority went further to say, "the reasonableness of the procedures followed in making these checkpoint stops makes the resulting intrusion on the interests of motorists minimal" up to and including "the stops and questioning at issue" "even if it be assumed that such referrals are made largely on the basis of apparent Mexican ancestry, we perceive no constitutional violation."[365] At the state level, Michigan State Police set up temporary Driving Under the Influence (DUI) checkpoints. Sitz et al. filed for injunctive relief against the checkpoints. The Court applied the three-part test from *Brown v. Texas*, 1) "weighing of the gravity of the public concerns served by the seizure," 2) "the degree to which the seizure advances the public interest," 3) "the severity of the interference with individual liberty." Under this balancing test, the vehicles were stopped for approximately 25 seconds; two arrests were made of the 126 vehicles checked. The 5-4 majority found the state's interest in preventing

[363] *LBS v. Baltimore*, 2 F.4th 330, 20 (2021)
[364] *United States v. Martinez-Fuerte*, 428 U.S. 543,560 (1976)
[365] *United States v. Martinez-Fuerte*, 428 U.S. 543, 562-563 (1976)

drunk driving and the minimal seizure that occurred was reasonable under the Fourth Amendment.[366] Conversely, in the almost nine months of surveillance over the city of Baltimore in 2016, there were,

> 21,243 calls to 911 inside the surveillance plane's coverage area. In total, McNutt's team submitted investigative briefings for 105 crimes, including 5 murders, 15 shootings, 3 stabbings, 16 hit-and-runs, and 1 sexual assault. In shootings and murder investigations alone, the company had tracked 537 targets, and had identified 73 people and vehicles thought to be "primary" suspects in these incidents. All told, leads collected by PSS had helped investigators advance at least 10 shooting investigations.[367]

In *Martinez-Fuerte* and *Sitz,* both petitioners endured what the court considered a reasonable seizure. The public good provided by WAPS was less injurious than a 25-second traffic stop. No stops are necessary, but significant public good was provided. WAPS is arguably the most constitutional investigative technology with a minimal level of intrusion when compared to traditional investigative methods and other new surveillance and investigative technologies. Even within a strict textual interpretation of the Fourth Amendment, WAPS would likely succeed because the collection does not concern private spaces which are particularly protected under "persons, houses, papers, and effects." It is doubtful that any other dragnet-level surveillance could be as effective with a such slight injury to the general public.

In conclusion, whether one evaluates WAPS under a strict textualist application of the Fourth Amendment or any fair balancing test to weigh the state's interest in combating crime against the public's protection from unreasonable searches, WAPS is constitutional. Existing precedent via *Dow Chemical* has already provided for advanced photographic technology to look down upon public and private property without constitutional concerns. *Dow Chemical* also clarified that even if such claims were applicable, they could only apply to Open Fields, which also hold no reasonable expectation of privacy. WAPS easily falls in line with the two-part test of *Katz*'s reasonable expectations of privacy compared to other persistent surveillance concerns.

---

[366] *Michigan Dept. of State Police v. Sitz*, 496 U.S. 448-449, 451-452 (1990).
[367] Arthur Holland Michel, Kindle Edition, Location 2917

The limited coverage is less persistent than the surveillance methods applied in *Knotts* and *Karo*. The advanced nature of WAPS technology does not violate the sanctity of private dwellings, which would restrain it under *Kyllo*'s general public use test. *Carpenter*'s warrant requirement does not apply because no single person is specifically being persistently surveilled without a documented call for assistance, specifically a 911 report. Even if WAPS were deployed with higher resolution cameras that could identify individuals, it could just as easily obscure the identifying characteristics of any individual caught under its watchful eye.

Chapter 5

WAPS is not Constitutional

The spirit of the Fourth Amendment does not permit WAPS by the government for policing purposes. The structure of the constitutional republic opposes such broad powers to the government, federal, state, or local. The unique nature of WAMI presents a new challenge to the Fourth Amendment, such that the police powers of states are not sufficient to extend a license for persistent surveillance against its own limited powers. The limitations of the federal government from such action have been successfully and properly incorporated against the States from deploying the same technology for the same invasive purposes. Because the Constitution requires the states to provide a republican form of government, consent must be gained from the people to legitimate any such operation, like WAPS. That is, statutory authorization explicitly describes what is permissible. Thus far, the exercises of persistent surveillance via *LBS* or *Tuggle* have been engaged in the "better to ask forgiveness than permission" model of investigation. Such an approach assumes the government has the power to engage in novel surveillance techniques before the legislature authorizes the alleged questionable actions by the state and its agents. Under *Grady v. North Carolina*,[368] consent is

[368] *Grady v. North Carolina*, 575 US __ (2015)

not sufficiently granted by passing legislation that would authorize such surveillance. *Grady* did not provide a rule to demonstrate what measure of consent is appropriate for persistent nonconsensual surveillance. Therefore, without an acceptable form of permission from the People, i.e., specified statutory authorization, the state may not conduct WAPS for law enforcement purposes.

In arguing for the constitutionality of WAPS, I have made a strict constructionist argument from existing precedents. By volume, more precedents can lead one to believe WAPS is more permitted than it is not. No Supreme Court precedents explicitly prohibit WAPS or any clear case with facts close enough to reliably predict what a strict constructionist interpretation of the Fourth Amendment might determine about WAPS. However, to interpret the lack of a prohibition against the government from conducting WAPS as permission is to misunderstand the Constitution of the United States. The initial fear the Founding Federalists had against a bill of rights was exactly that kind of interpretation of the Constitution.

> I go further, and affirm that bills of rights... are not only unnecessary in the proposed Constitution, but would even be dangerous. They would contain various exceptions to powers not granted; and, on this very account, would afford a colorable pretext to claim more than were granted. For why declare that things shall not be done which there is no power to do?[369]

To abandon the spirit of the Constitution in exchange for a series of articulated opinions shared by numerous jurists earnestly seeking to define a subjective standard in the Fourth Amendment is to rely upon mere "parchment barriers."[370] Those who drafted them, they knew such measures were insufficient. These weak barriers were not supposed to be the bulwark of protection against encroaching authority. The active operation of the constitutional structure through the People was supposed to be the mitigating force from tyranny. Some might argue that the development of rational basis review and its subsequent interpretations abandoned the limitations of the federal government over fifty years ago,[371] in as far as Fourth Amendment

[369] Hamilton, Alexander. The Federalist #84
[370] Madison, James. The Federalist #48
[371] *Williamson v. Lee Optical Co.*, 348 U.S. 483 (1955)

jurisprudence applies, our security against unreasonable searches and seizures is still recognized as a fundamental right.

The Fourth Amendment is broader than the Court has judged according to the "zones of privacy"[372] found across the text. However, most specifically in the Ninth Amendment, "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." The original understanding of the Constitution was to protect the People from the Federal government. Explicitly from 1833 to 1925, that understanding meant the Bill of Rights was effective against only the Federal government, not the State governments.[373] The incorporation of the Fourth Amendment against the States extended the burden of the supreme law of the land to secure the people from unreasonable searches and seizures properly. In Federalist 84, Hamilton explained his concerns with a bill of rights, namely that rights not listed would shift the government's understanding from the structure of the Constitution, which enumerated its rights, to the shortlist provided in the Bill of Rights.

It is in the government's legitimate interest to seek to protect the people. This goal is one of the most basic tasks that justify forming civil society. However, the republican form of government guarantee in Article IV requires the government not to assume powers not given to it by the People. Jurists have debated who "The People" are in constitutional interpretation ranging from the general populace of the nation to the state legislatures.[374] This chapter suggests that WAPS should not be deployed before the people consent to such action, absent exigent circumstances. On this point, WAPS is in a particularly unconstitutional position. Holland Michel and local reporters have consistently reported that law enforcement officials across jurisdictions are reluctant to disclose to their constituents or elected officials about spy

[372] *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965)
[373] *Barron v. Baltimore*, 32 U.S. (7 Pet.) 243 (1833) and *Gitlow v. New York*, 268 U.S. 652 (1925).
[374] *District of Columbia v. Heller*, 554 U.S. 570 (2008), Justice Scalia's majority opinion understood "the People" to be the general populace, Justice Stevens' dissent argued "the People" referred to the State government.

technology being used to combat crime.[375] Using technology against the people without their consent is an affront to limitations built into representative governments. The next question on appeal from the spirit of the Constitution will be, "if WAPS is within the purview of the Necessary and Proper Clause?" A strict application of *McCulloch v. Maryland* would find no necessary or proper task provided in Article I that might justify such operations, particularly concerning state and local use, which are the limitations of this work.[376] The issue of using WAPS for national security purposes is for a different analysis altogether.

Thus far, the case has been primarily made against federal government officials using WAPS for law enforcement because the argument has been based on the federal constitution. Does the same standard exist for state governments to deploy whatever technologies they deem necessary? No, from two places. The right to privacy is a Natural Right established in the Social Contract. Those inclined to read the Declaration of Independence into the Constitution would recognize that the Constitution upholds the principles of "life, liberty, and the pursuit of happiness." One does not need a graduate-level understanding of John Locke's philosophy or Justice Brennan's jurisprudence to understand "liberty" to include a basic sense of personal

---

[375] Arthur Holland Michel, Kindle Edition, Locations 1339,1445, 1459, 2987, and 3541.;Rector, Kevin, "Cummings: Commissioner Davis 'apologized profusely' for not disclosing surveillance program," Baltimore Sun, https://www.baltimoresun.com/news/crime/bs-md-ci-cummings-davis-meeting-20160902-story.html, accessed August 6, 2020.; Farivar, Cyrus, "FBI would rather prosecutors drop cases than disclose stingray details," Ars Technica, April 7, 2015, https://arstechnica.com/tech-policy/2015/04/fbi-would-rather-prosecutors-drop-cases-than-disclose-stingray-details/, accessed August 6, 2020.; Moran, Greg, "Are those government spy planes overhead?" San Diego Tribune, April 8, 2016 https://www.sandiegouniontribune.com/news/data-watch/sdut-spy-planes-2016apr08-htmlstory.html accessed August 6, 2020.; Cenciotti, David, "Online flight tracking exposes FBI Aerial Surveillance over San Bernardino Mosque after Terrorist Attack," The Aviationist, December 5, 2015, https://theaviationist.com/2015/12/05/fbi-activity-san-bernardino-attack/ accessed August 6, 2020.; Muntean, Pete and Wallace, Gregory, "US government spy planes monitored George Floyd protests," June 11, 2020, CNN, https://www.msn.com/en-us/news/us/us-government-spy-planes-monitored-george-floyd-protests/ar-BB15lIme?ocid=sf accessed August 6, 2020.; Woolf, Nicky, "2,000 cases may be overturned because police used secret Stingray surveillance," The Guardian, September 4, 2015, https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance accessed August 6, 2020.; Grauer, Yael, "Security News This Week: The NYPD Doesn't Want You to Know About Its X-Ray Spy Vans," Wired, October 17, 2015, https://www.wired.com/2015/10/security-news-this-week-the-nypd-doesnt-want-you-to-know-about-its-x-ray-spy-vans/ accessed August 6, 2020.

[376] *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316 (1819)

privacy. Per Natural Law theory, such principles were merely recognized by the Bill of Rights, not established by them. The whole body of law should seek to align itself with those preexisting rights.[377] Additionally, the applicable portions of the Bill of Rights, which restrain government practices beyond natural rights, have been incorporated against the states.

The argument against the constitutionality of WAPS in the Fourth Amendment is best argued from an appeal to Natural Rights. More specifically, a negative right that requires no proactive action by the state to grant, but it does prompt a restraint from depriving the people of the right. In the words of then Professor Louis Brandeis, "[T]he right to be let alone." Brandeis and Warren published one of the earliest American legal articles discussing the existence of the right to privacy.[378] To be fair, the argument was not presented as a natural right but as a property right. The article was explicitly directed towards the property lost from gossip exposing people's secrets, an early treatise against the paparazzi. The "penumbra" of the Fourth Amendment to cover more than the strict text was not introduced until Justice Holmes's dissent in *Olmstead v. United States*.[379] It should also be acknowledged that the "right to be let alone," used in 1928, was far more narrow than what is being proposed here. This is because it was contemporary to the prophetic dissent from Justice Brandeis in *Olmstead*. A case where the majority of the Court ruled warrantless wiretaps were not a violation of the Fourth Amendment or Fifth Amendment in the most strict textual sense. In one of his most famous dissenting opinions, Justice Brandeis cautioned,

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related

[377] Martin Luther King Jr., "Letter from Birmingham Jail," August 1963, accessed January 15, 2018, https://www.csuchico.edu/iege/_assets/documents/susi-letter-from-birmingham-jail.pdf
[378] Samuel Warren and Louis Brandeis, "The Right of Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890): 193.
[379] *Olmstead v. United States*, 277 U.S. 438, 469 (1928)

> sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[380]

To those familiar with the predictive capabilities of search engines and social media algorithms, Justice Brandeis' caution sounds more prophetic each day. This strikingly accurate forecast for the 21st century was rumored to result from an apparent misunderstanding of new 20th-century technology, television. Justice Brandeis was under the impression that this new technology-enabled video conferencing, not one-way broadcasts. This mistake has informed generations of legal scholars of future challenges. It also challenges those who belittle the wisdom of previous generations on the grounds of their chronological irrelevance. In *Olmstead*, Justice Brandeis did not argue for privacy from a property right position as he did thirty-eight years prior; instead, he argued it based on the limited structure of the government.

> We have likewise held that general limitations on the powers of Government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the States from meeting modem conditions by regulations... Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.[381] ...Its general principles would have little value and be converted by precedent into impotent and lifeless formulas. Rights declared in words might be lost in reality.[382]

Though the right to privacy in American jurisprudence did not originate in Natural Rights, proper reflection makes such an application appropriate and more accurate.

Because the role and concept of Natural Rights in the Constitution are far from settled, a more effective interpretive method to uphold the people's unenumerated rights is found in the individual's liberty interests via the Due Process clause. "The Fourth Amendment protects people, not places."[383] "Fourth Amendment rights are personal rights."[384]

> In every case that comes before this court, therefore, where legislation of this character is concerned and where the protection of the Federal Constitution is sought, the question necessarily arises: Is this a fair, reasonable and appropriate

---

[380] *Olmstead v. United States*, 277 U.S. 438, 474 (1928)
[381] *Olmstead v. United States*, 277 U.S. 438, 472 (1928)
[382] *Olmstead v. United States*, 277 U.S. 438, 473 (1928)
[383] *Katz v. United States*, 389 U.S. 351 (1967)
[384] *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978)

> exercise of the police power of the State, or is it an unreasonable, unnecessary and arbitrary interference with the right of the individual to his personal liberty.[385]

These excerpts from landmark cases describe the spirit of the Fourth Amendment. The protection against unreasonable searches and seizures was not an arbitrary goal. It responded to the previous regime, which used its power to search and seize at will. The People were at the mercy of the state and its agents. Arguments based on liberty claims are arguably some of the most controversial landmark decisions of the recent century. Lochner being the first to declare such an audacious concept, limited police powers.

> There are, however, certain powers, existing in the sovereignty of each State in the Union, somewhat vaguely termed police powers... Those powers, broadly stated and without, at present, any attempt at a more specific limitation, relate to the safety, health, morals and general welfare of the public. Both property and liberty are held on such reasonable conditions as maybe imposed by the governing power of the State in the exercise of those powers, and with such conditions the Fourteenth Amendment was not designed to interfere.[386]

"The future is their care and provision for events of good and bad tendencies of which no prophecy can be made. In the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be."[387] There is something unique about the breadth of information that can be gathered about a person with WAPS. In *Carpenter*, the majority opinion was based on the "unique nature of cell phone location information." *Griswold*'s "zones of privacy" were not so limited to only be private property, where the Court has been clear to protect, but it also included "the privacies of life."[388] Reliance on penumbras and emanations is a weak basis for making a constitutional argument, but so is the whole concept of privacy in American jurisprudence. As flawed as the emanations and penumbras may be, they provided the basis for several of the last half-century's most significant (and controversial) liberties. With this application, one can faithfully claim with a reasonable connection to the text that it is being referred to such that "it is a Constitution we are expounding."[389]

---

[385] *Lochner v. New York*, 198 U.S. 56 (1905)
[386] *Lochner v. New York*, 198 U.S. 45, 53 (1905)
[387] *Olmstead v. United States*, 277 U.S. 438, 473 (1928), Justice Brandeis' dissent
[388] *Boyd v. United States*, 116 U.S. 616, 630 (1886)
[389] *McCulloch v. Maryland*, 17 U.S. 407 (1819)

Because of the incorporation of the Fourth Amendment, this also extends to the States. Although the Founders did not correctly conceive of states violating the rights of the People despite the plain example of involuntary servitude before them, the incorporation of the Fourth Amendment should be used to guard the people against their own officials, elected or not. The argument concerning the just representation of the people by our present elected officials at the state and federal levels is best reserved for another time. As mentioned in the previous chapter, *Jones* rejected the Mosaic Theory; however, it did not do so because the majority opinion rejected placing the GPS device in the first place. The Court effectively "punted" the question about the nature of the persistent data collection. The DC Circuit case, *Maynard,* was consolidated with *Jones* and thoroughly fleshed out the Mosaic Theory. The unanimous opinion written by Judge Ginsburg has not been explicitly accepted or rejected by the Supreme Court. Judge Ginsburg challenged the understanding under *Knotts* that Maynard's movements were actually "exposed to the public."[390] Simply because one drives a vehicle in public does not necessarily constitute exposure of the totality of movement over the month he was surveilled. It is reasonable that a member of the public would not expect to be followed around for a month with someone annotating every movement. Justice O'Connor's concurring opinion acknowledged a similar argument presented in *Florida v. Riley*, a case very similar to *Ciraolo*, in which the flight paths of passenger aircraft were not necessarily equal to police helicopters flying at 400 feet.[391] This was important because of the second condition of Justice Harlan's concurrence in *Katz*, "that the expectation be one that society is prepared to recognize as "reasonable."[392] In *Florida v. Riley*, the plurality viewed the surveillance as acceptable under the Fourth Amendment because the helicopter did not violate FAA regulations. Justice O'Connor's concurrence sharply criticized the plurality's reliance on safety regulations being used to justify

[390] *United States v. Maynard*, 215 F.2d 336 (D.C. Cir. 1954) 94 U.S. App. D.C. 347, 21-30.
[391] *Florida v. Riley*, 488 U.S. 445, 454-455 (1989)
[392] *Katz v. United States*, 389 U.S. 361 (1967)

or set limitations on surveillance operations. “The fact that a helicopter could conceivably observe the curtilage at virtually any altitude or angle, without violating FAA regulations, does not in itself mean that an individual has no reasonable expectation.”[393] Justice Brennan’s dissenting opinion also highlighted the same point as Justice O’Connor, “the opinion relies almost exclusively on the fact that the police officer conducted his surveillance from a vantage point where, under applicable Federal Aviation Administration regulations, he had a legal right to be.”[394]

WAPS is unconstitutional because it would lack sufficient consent. Suppose WAPS was to be approved by properly elected officials. Most city councils can pass a resolution at will at the city government level. The degree of practiced representation is more significant than for federal offices. This is because the actions of local legislators will directly affect their constituents, and the amount of information available from city governments is less than that of state and federal bodies. City governments tend to have less sophisticated infrastructure and digital networks to adequately host transparent government operations. A real-time analogy as an example, the release of police body camera video is often made so by law enforcement agencies or the district attorney. Cities do not make available the totality of police bodycam video without specific records requests at best. Currently, only California, Florida, and North Dakota have laws governing the disclosure of police body camera video.[395] This is an issue of consent because the People cannot provide informed consent to what they do not know, state officials, or the voting populace. I frame this as a form of informed consent with a higher standard than conventional consent because of the potential harm that can be inflicted upon the People if they do not know what WAPS is.

---

[393] *Florida v. Riley*, 488 U.S. 445, 454 (1989)
[394] *Florida v. Riley*, 488 U.S. 445, 456 (1989)
[395] State Law Enforcement Body Camera Policies, Electronic Privacy Information Center, Epic.org, https://epic.org/state-policy/police-cams/#:~:text=California%20considers%20body%2Dcamera%20videos,privacy%20rights%20of%20individuals%20depicted. Accessed August 11, 2020.

As applied to potential state surveillance, the Court has addressed the concern of persistent non-consensual aerial location monitoring in *Grady v. North Carolina*. The Court acknowledged that the non-consensual nature of the surveillance was a clear violation of precedent, relying on *Jones*. The brief Per Curiam opinion found a lifetime requirement to wear a satellite-based monitoring (SBM) device of a repeat convicted sex offender violated his Fourth Amendment rights.[396] As with *Jones*' analysis, the factual differences of an SBM tracking against WAPS are significant, but the ruling still applies to the constitutional condition of WAPS, specifically concerning consent. The key difference was that the SBM for Grady was a fully persistent lifetime condition and a consequence of his convicted crimes. Grady's freedom from incarceration was not conditioned that he submit to the SBM. Grady was convicted in 2006, released in 2009, then convicted again for failing to register as a sex offender. This conviction was his third over ten years, incontestably classifying him as a recidivist.[397] Senate Bill 53 was passed in 1995, authorizing the North Carolina Sex Offender Registry.[398] In 2006, North Carolina law mandated that those on the registry classified as recidivist offenders be subject to lifetime, persistent, non-consensual SBM.[399] Post-*Grady*, the registration continues to exist, but the lifetime requirement was reduced to 30 years with the possibility of lifetime registration under certain aggravating conditions.[400] The Court rejected North Carolina's claim that a lifetime non-consensual persistent surveillance was consistent with the Fourth Amendment, citing *Jones*.[401] Although an SBM was an uncommon device, *Kyllo* was not mentioned by the Court to pose a general public use challenge to technology that otherwise revealed information only

[396] *Grady v. North Carolina*, 575 U. S. ____ (2015)
[397] Roy Cooper and Joseph Finarelli, "*Grady v. North Carolina* Brief of Respondent in Opposition," http://sblog.s3.amazonaws.com/wp-content/uploads/2015/03/Grady-states-response.pdf accessed August 11, 2020. 1-3.
[398] Senate Bill 53, North Carolina General Assembly 1995-1996 Session, https://www.ncleg.gov/BillLookUp/1995/S53 accessed August 12, 2020.
[399] *State v. Blue*, 246 N.C.App. 259 (2016); N.C. Gen.Stat. § 14–208.40
[400] North Carolina General Statutes § 14-208.6A.
[401] *Grady v. North Carolina*, 575 U. S. ____ (2015), 2-3.

gathered by entering a dwelling. Compared to SBM or CSLI data, WAPS, under the Baltimore proposal, was not persistent surveillance unless the asset was persistently operating. The mere use of persistent surveillance technology is insufficient to claim that persistent surveillance is underway when operations are intermittent. The surveillance is limited to the collection area of up to 64 square miles during daylight hours. If one leaves the coverage area, they will experience full liberty, unlike the SBM, which will track one's movements anywhere on the planet. Additionally, the individual with the SBM device has been identified. In contrast, those under the dragnet of WAPS can remain anonymous until the data is cross-correlated with other surveillance or public records.[402]

The common factor between WAPS and *Grady* is questionable non-consensual surveillance by the state. From whom does consent originate? Is it the parties under which surveillance is performed or the representative bodies who make the law? In *Grady*, the North Carolina legislature consented to the consequences of criminal behavior, wherein the SBM tracking device was among the consequences. To date, no state legislature has explicitly authorized a similar scheme of surveillance permitted via statutory authorization. The consent issue should not depend on the Court's acknowledgment that a search has or has not occurred. WAPS is an active system that immediately begins to affect those being surveilled. In our republican form of government, consent is accepted by the proper actions of elected legislators dutifully drafting laws that follow the procedural process that makes a law from a bill. In *Grady*, the Court did not accept the extent to which the legislature authorized SBM surveillance, thus demonstrating the balancing tests within the state's authority against what would be considered a special need. In the key passages describing the reasoning, the lack of consent to the SBM was a significant factor. The judgment by the Court presents a unique challenge which opponents of WAPS may also claim. The concern over consent assumes any further

[402] Arthur Holland Michel, Kindle Edition, Location 1170.

deployment of WAPS over domestic locations is transparent enough to inform elected officials of its operations. Under *Grady*, such a standard is insufficient. However, under *Grady*, the lack of consent may prohibit the state's exploitation of electronic-based data, search or not. It is also important to note Per Curiam's opinions' role in broader jurisprudence. They tend to hold less weight in the hierarchy of precedents. However, the Court's ruling in *Grady* does present a significant hurdle to the constitutionality of new surveillance technologies, WAPS included.

In summary, the structure of the Constitution and the spirit of the Fourth Amendment does not permit WAPS. The justification for its constitutionality relies on the assumption that what is not prohibited by the government is permissible. This approach is a fundamental inverse of the design and structure of the Constitution. This traditional understanding of the Constitution is more faithful to the text than the long list of well-developed precedents presented in the previous chapter. Because the federal government is limited, the incorporation of the Fourth Amendment against the states also brings those same limits to government power. Among the unique challenges of WAPS is determining "to whom and to what degree should consent to surveillance be applied?" This is the same argument from the spirit of the Fourth Amendment more generally, but with the support of recent precedent to make the emanations incarnate.

Chapter 6

Baltimore's AIR Program, a Case Study

Following the Reel article, members of the public and elected officials alike voiced significant concerns when the city sought to establish the AIR program. Reel's reporting of deliberate and purposeful secrecy of the WAPS pilot program in 2016 by law enforcement officials from any elected city officials reasonably prompted concern for the 2020 program's opponents. In response, specific research requirements were necessary for the AIR program to launch, including community outreach survey research by Baltimore University, legal analysis

from New York University's Policing Project, and the AIR program's effectiveness assessed by Rand Corporation.[403]

This chapter will focus on summarizing and analyzing *LBS v. Baltimore*. This analysis focuses primarily on the United States District Court for the District of Maryland and the United States Court of Appeals for the Fourth Circuit. In these courts, the arguments and opinions were most applicable to understanding the Fourth Amendment concerns of WAPS. LBS ended at the Fourth Circuit en banc panel, wherein Chief Judge Gregory wrote the majority opinion. Chief Judge Gregory's majority opinion was largely intact from his dissent when the case came before the three-judge panel. The focus on the three-judge panel instead of the fifteen-judge panel was due to the facts at the time of the proceedings. When the en banc panel held oral arguments, the concerns over the AIR program were about the remaining archived WAPS data. The AIR program concluded its six-month pilot period. Mayor Scott promised not to restart it.[404] The ripeness of the case had passed to the degree that a significant portion of the en banc panel's oral argument focused on the mootness of the case.[405]

From May to October 2020, Baltimore Police Department contracted Persistent Surveillance Systems three WAPS-equipped aircraft to fly over the city of Baltimore during daylight hours.[406] Weather permitting, each aircraft was to fly at least forty hours per week.[407] The terms of the Memorandum of Understanding (MOU) limited the PSS analysis to reports of

---

[403] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 5.
[404] Opilo, Emily. "Spy Plane Not Likely to Fly over Baltimore Again, Mayor Says." baltimoresun.com, December 28, 2020. https://www.baltimoresun.com/politics/bs-md-pol-brandon-scott-interview-20201228-ti75hqctsffgrbyggpzdz2xtgm-story.html.
[405] Oral Arguments, *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc) accessed April 15, 2021, https://www.ca4.uscourts.gov/oral-argument/listen-to-oral-arguments
[406] Police Commissioner Michael S. Harrison to The Honorable President and Members of the Board of Estimates, March 17, 2020, Baltimore Police Department, Professional Service Agreement Acceptance (Memorandum of Understanding), Exhibit A, 18.
[407] Police Commissioner Michael S. Harrison to The Honorable President and Members of the Board of Estimates, March 17, 2020, Baltimore Police Department, Professional Service Agreement Acceptance (Memorandum of Understanding), Exhibit A, 19.

"murder, non-fatal shootings, armed robberies, and car-jackings."[408] The MOU required several limitations for the program to be used. Infrared and night vision technology was not permitted; infrared cameras can see through weather and low light conditions but are grayscale images. The electro-optical camera permitted was similar to conventional cameras in civilian use.

Additionally, the resolution of the images could not be greater than one square meter per pixel, further preventing "any identifiable characteristic including an individual's ethnicity, sex, or clothing or a vehicle color, make, model or license plate." The analysts could only zoom-in to specific locations upon request from the Computer Aided Dispatch or Shotspotter systems used by the BPD.[409] The analysts were also linked to the Citiwatch Ground Based Camera network, which consisted of approximately eight hundred subsidized cameras on private property.[410] Unanalyzed data could be stored for up to forty-five days and analyzed data used in investigations was compiled into packets and made a part of the permanent case file.[411] Like the 2016 pilot program, the AIR program was funded by Arnold Ventures, a criminal justice philanthropy.[412]

LBS is a "grassroots think-tank which advances the public policy interest of Black people, in Baltimore."[413] In April 2020, with the support of ACLU Baltimore, they requested a

---

[408] Police Commissioner Michael S. Harrison to The Honorable President and Members of the Board of Estimates, March 17, 2020, Baltimore Police Department, Professional Service Agreement Acceptance (Memorandum of Understanding), 18.
[409] Police Commissioner Michael S. Harrison to The Honorable President and Members of the Board of Estimates, March 17, 2020, Baltimore Police Department, Professional Service Agreement Acceptance (Memorandum of Understanding), Exhibit A, 19.
[410] Kendall Green, "'That's an Extra Eye': Citiwatch Camera Improvements Crucial to Curbing Crime," WMAR (WMAR, May 20, 2022), https://www.wmar2news.com/news/local-news/thats-an-extra-eye-citiwatch-camera-improvements-crucial-to-curbing-crime.; Police Commissioner Michael S. Harrison to The Honorable President and Members of the Board of Estimates, March 17, 2020, Baltimore Police Department, Professional Service Agreement Acceptance (Memorandum of Understanding), Exhibit A, 20.
[411] Police Commissioner Michael S. Harrison to The Honorable President and Members of the Board of Estimates, March 17, 2020, Baltimore Police Department, Professional Service Agreement Acceptance (Memorandum of Understanding), 2.
[412] "About." Arnold Ventures. Accessed June 16, 2022. https://www.arnoldventures.org/about.
[413] Leaders of a Beautiful Struggle, "Leaders of a Beautiful Struggle About Us," accessed November 10, 2021, https://www.lbsbaltimore.com/about-us/.

temporary injunction against the AIR program in the United States District Court of Maryland. The complaint claimed the extensive surveillance would disrupt their ability "to associate with others, free from unwarranted government scrutiny," essential characteristics necessary for their political activity and advocacy.[414] This line of reasoning originated from Neil Richards.[415] LBS claimed the AIR surveillance was "inescapable… short of never leaving the home when the planes are in the air."[416] Because of the expansive surveillance, it would inevitably reveal private information of those surveilled, including the movements in protected curtilages. Although the AIR cameras could not identify individuals from the aerial surveillance alone, because the AIR program was designed to be integrated with other BPD databases, the aerial surveillance could be used to easily "deduce identity."[417] One of the named plaintiffs, Ms. Bridgeford, was concerned an individualized report would be built about her because her duties with LBS required her to visit murder scenes and be in the vicinity of violent crimes. Such surveillance was argued to violate her reasonable expectation of privacy.

The complaint under 42 U.S.C. § 1983 was twofold. First, it described the AIR surveillance as a search and thus failed the requirements of individualized suspicion, probable cause, or warrant requirements. Second, the constant and inescapable monitoring infringed on associational freedoms. The sought declaratory relief was an admission from the Baltimore Police Department (BPD) the AIR program violated the First and Fourth Amendment rights of LBS, a permanent injunction against the AIR program and any agent involved in operating it, expunged records of plaintiffs created by the AIR program, and attorney fees. The Maryland

[414] "Leaders of a Beautiful Struggle v. Baltimore City Police Department," ACLU of Maryland, June 24, 2021, https://www.aclu-md.org/en/cases/leaders-beautiful-struggle-v-baltimore-city-police-department.
[415] Neil Richards, "The Dangers of Surveillance," 26 Harvard Law Review 1934, 2013, accessed May 3, 2022, https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/.
[416] Neil Richards, "The Dangers of Surveillance," 26 Harvard Law Review 1934, 2013, accessed May 3, 2022, https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/.
[417] Neil Richards, "The Dangers of Surveillance," 26 Harvard Law Review 1934, 2013, accessed May 3, 2022, https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/.

Federal District Court rejected the requested temporary restraining order (TRO) in *LBS v. Baltimore*.

Judge Richard Bennett noted the intermittent periods of surveillance and the anonymity of those surveilled as significant contributing factors to the denial of the injunction.[418] Plaintiffs of any TRO must establish a "heavy burden to show that they are entitled to a preliminary injunction."[419] The extraordinary burden necessary to overcome a TRO notwithstanding, Judge Bennett based the analysis of the AIR program's acceptability on the guarantee that personal identifying information (PII) was not possible to collect from the WAPS operated by PSS. The imagery would not be more detailed than a single person being represented by a single pixel, a point mentioned five times in the short opinion. The limited resolution prevented features such as race, sex, clothing, or any potential identifying characteristics from being captured by the AIR program. Part of the initial terms of the AIR program included separate evaluations from Morgan State University RAND Corporation on the program's crime-fighting efficacy, a public perception study by the University of Baltimore, and a "civil rights and civil liberties audit" by the New York School of Law. Upon the rejection of the TRO, the AIR program commenced from May 1st to October 31st.[420]

Under the city's Memorandum of Agreement (MOA), specific limitations were established for the AIR operations. Those limitations included: no night flights; the inability to collect PII; acknowledgment of lost positive identification anytime a person entered a building; no additional zoom, infrared, or telephoto technologies; imagery analysts could only access the data following a notification relating to murder, non-fatal shooting, armed robbery or carjacking; only forensic tracking was permitted; and any images used in investigations would be given to prosecutors and defense counsel; otherwise the data would be deleted after 45 days.[421]

---

[418] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 456 F.Supp.3d 699 (2020)
[419] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 456 F.Supp.3d 699 (2020)
[420] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020)
[421] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020)

Judge Bennett upheld the constitutionality of the AIR program citing the Flyover Cases, *Dow Chemical* in particular, because the detail of the imagery was more detailed than it is in this WAPS.[422] Judge Bennett highlighted how in *Dow Chemical*, the EPA used the "finest precision aerial camera available"[423] capable of identifying wires "as small as ½-inch in diameter,"[424] much greater detail than what PSS was capable of. Judge Bennett also cited *Ciraolo* and *Riley* to uphold the non-search nature of flyovers over Open Fields. AIR surveillance did not "penetrate walls," "record confidential discussions," reveal "intimate details" associated with a person's home, or "disturb the use of a person's property."[425] Judge Bennett considered the AIR surveillance less intrusive than pole cameras which recorded "bodily movements, observe facial expressions, record in real-time, zoom-in on suspicious activities, or record illegal activities near the curtilage of the home or even in open fields."[426] Such warrantless, long-term cameras have been upheld in the First, Fourth, Fifth, Sixth, Seventh, and Tenth Courts of Appeals.[427] Judge Bennett did not believe *Carpenter* applied because the majority opinion did not "call into question conventional surveillance techniques and tools, such as security cameras."[428]

The reliance Judge Bennett gave on the limited resolution of the WAPS operated by PSS was crucial in his analysis. The Hawkeye Wide Area Imaging System deployed by PSS was only 192 megapixels.[429] The area of a single pixel under PSS practices was approximately three square feet. In comparison, the optical sensors on ARGUS-IS are 1.8 gigapixels. The Advanced Wide FOV Architectures for Image Reconstruction and Exploitation (AWARE) camera

[422] *Dow Chemical Co. v. United States*, 536 F. Supp. 1355,1357 (1982)
[423] *Dow Chemical Co. v. United States*, 476 U.S. 230 (1985)
[424] *Dow Chemical Co. v. United States*, 476 U.S. 238 (1985)
[425] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 456 F.Supp.3d 699 (2020)
[426] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 456 F.Supp.3d 699 (2020)
[427] *United States v. Bucci*, 582 F.3d 108, 116-17 (1st Cir. 2009); *United States v. Vankesteren*, 553 F.3d 286, 291 (4th Cir. 2009); *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); *United States v. Houston*, 813 F.3d 282, 285-86 (6th Cir. 2016); *United States v. Jackson*, 213 F.3d 1269, 1276, 1280-81 (10th Cir.); *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021)
[428] *Carpenter v. United States*, 138 S. Ct. 2220 (2018)
[429] McNutt, Ross.

made by DARPA and Duke University has a 40 gigapixel resolution.[430] ARGUS-IS claims to be able to read vehicle license plates from an altitude of 20,000 feet. Although ARGUS-IS still has less detail than the camera used in *Dow Chemical*, the wide-area function of ARGUS-IS and other high-resolution WAPS are likely to manifest the "dragnet-type law enforcement practices" mentioned in *Knotts*.[431] PSS could tune their WAMI camera to have a higher resolution with a smaller coverage area. McNutt believed extending the surveillance perimeter was more prudent and constitutional than increasing the detail.[432] Such a course of action was more prudent to remain consistent with the second portion of Katz's reasonableness standard.[433]

The bright line proposed to separate the "dragnet-type law enforcement practices" in terms of WAPS is Personal Identifying Information (PII). PII has several definitions from relevant government sources and statutes. The Department of Homeland Security describes PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual." Additionally, sensitive PII "includes Social Security Numbers, driver's license numbers, Alien Registration numbers, financial or medical records, biometrics, or a criminal history."[434] The Violence Against Women Act of 1994 described PII to include several levels of personal information, the most generic being "racial or ethnic background, or religious affiliation."[435] Strictly speaking, the only PII vulnerable to WAPS in high-resolution imagery would be a clear picture of a person's face, similar to what is present

---

[430] Arthur Holland Michel.
[431] *United States v. Knotts*, 460 U.S. 284 (1983)
[432] Craig Timberg, "New Surveillance Technology Can Track Everyone in Area for Several Hours at a Time," Washington Post (Feb. 5, 2014), accessed 28 July 2021, retrieved from 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.
[433] *Katz v. United States*, 389 U.S. 361 (1967)
[434] "What is Personally Identifiable Information," Department of Homeland Security, accessed October 6, 2022 https://www.dhs.gov/privacy-training/what-personally-identifiable-information.
[435] Violence Against Women Act of 1994, 34 U.S. Code § 12291 "(A) a first and last name; (B) a home or other physical address; (C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number); (D) a social security number, driver license number, passport number, or student identification number; and (E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual." https://www.law.cornell.edu/uscode/text/34/12291

on an identification card. PII would not necessarily be defined so broadly as to include general clothing descriptions. If or when sufficiently high-resolution cameras for WAPS are considered, the program would have to proactively obscure the identifying information until a warrant could be obtained to unlock the detailed resolution.

It is unreasonable to reliably identify street addresses without first analyzing raw WAPS data. The raw data refers to zoomed-out city-wide imagery. The raw data form of WAPS is similar to looking out a window of an aircraft. One can see the city, but the limits of our vision preclude seeing anything specific. The wide-area coverage of the WAPS and the resolution make it worthwhile. One can zoom in on specific areas to observe vehicles or people. In the case of the AIR program, it is essential to emphasize that a single person is a single pixel. The mere collection of WAPS data cannot identify anyone or anything in a law enforcement capacity. The value is in the analysis stage, which is zooming in to specific areas and tracking pixels/persons of interest. As with the AIR program, a report was required for an analyst to zoom in on any location. Rogue analysts could not zoom in on random locations without a legitimate purpose. Because of this limitation, which should be upheld for any law enforcement use of WAPS, personal location information is not accessible before probable cause is established. In addition, masking the residential addresses of persons of interest would be easier than blurring high-resolution imagery. The raw WAPS data needs to be synchronized with reference map data to identify any specific location. On software programs like ArcGIS or GoogleEarth, the WAPS data is a separate layer from the reference map data, and the analyst must reconcile the two. Once the event or person of interest is initially identified for tracking, with a mouse click or two, the analyst can deactivate the reference map layer for the report. Even if a street address is identified, potential occupants could not be identified without access to additional databases. A single pixel cannot be reasonably used to positively identify any person for an investigation.

The ACLU and LBS appealed to the US Court of Appeals Fourth District. Chief Judge Roger Gregory, Judge Paul Niemeyer, and Judge J. Harvie Wilkinson III composed the panel. Judges Wilkinson and Niemeyer denied the appeal, and Chief Judge Gregory dissented. By the time the opinion was released, funding and political leadership changes had already concluded the AIR program. The complaint then concerned the archived data being used in active criminal cases.

Additionally, the "civil rights and civil liberties audit" commissioned as part of the pilot program was completed. The preliminary efficacy analysis by RAND Corporation was completed in January 2021. The panel rejected Judge Bennett's denial of standing but also upheld the "clear showing" necessary for a preliminary injunction that their case would likely succeed on the merits. The vague but reasonable claims in the complaint failed to meet the three requirements for a TRO; (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of equities favors the grant for relief, and (4) the injunction was in the public interest.[436]

The majority evaluated the AIR program on the reasonable expectation of privacy standards and balanced it with the jurisprudence on Programmatic Searches.[437] These tests provided a subjective and objective component of evaluation in their decision by asking if "the government action arbitrarily invaded the "privacies of life" and if courts should be wary of "a too permeating police surveillance"?[438] The primary limiting rule on the individual's expectation of privacy was cited by *Katz*, "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[439]

---

[436] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020)
[437] *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990); *United States v. Flores-Montano*, 541 U.S. 149 (2004); *Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318 (2012).
[438] quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)
[439] *Katz v. United States*, 389 U.S. 347, 351 (1967).

Because the imagery could not be processed until the specific violent crimes were reported, as with Judge Bennett's analysis, Judge Wilkinson writing for the majority, prioritized the anonymity of the subjects surveilled, the limitations of the single-pixel, as the most significant grounds to uphold the lower court's ruling. When combined with the programmatic limits per the MOA, the majority found the AIR program to be less intrusive than other forms of aerial surveillance. Unlike the Flyover Cases, the wide-area photos could not identify backyard contents, even when zoomed in. The majority rejected the briefs and complaints which challenged the broader set of tools used by BPD to include the ground-level Citiwatch camera system and automated license plate readers in conjunction with the AIR surveillance. In agreement with Judge Bennett, the majority used similar applications of *Dow Chemical*, *Ciraolo,* and *Florida v. Riley*.[440]

The panel denied that the AIR surveillance was long-term. Because of the break in coverage at night and any time a subject entered a building, a multi-day positive identification could not be maintained as it was in *Carpenter*, *Jones*, and *Knotts*. Also, in agreement with Judge Bennett, the majority did not believe *Carpenter* could be applied, "*Carpenter* simply does not reach this case because CSLI offers a far more intrusive, efficient, and reliable method of tracking a person's whereabouts than the AIR pilot program."[441] Factors that distinguished *Carpenter* from being applied also included the effort of using CSLI versus AIR analysis. Phone carriers could readily provide CSLI to track an individual; with AIR, analysts had to spend hours to "tag a person of interest and reconstruct a couple of hours of his public movements."[442] The majority concluded Part A of their decision by emphasizing the built-in controls specific to the AIR program, which maintained its constitutionality. Had the AIR program performed 24-hour collection and the capacity to identify specific people quickly, the majority would have ruled

[440] *California v. Ciraolo*, 476 U.S. 207 (1986), *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), and *Florida v. Riley*, 488 U.S. 445 (1989)
[441] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 14.
[442] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 15.

differently. Such capabilities would require much higher resolution cameras and integrated facial recognition capabilities.

According to the majority, the AIR program was not an unreasonable Programmatic Search. The AIR program met the panel's standard of reasonableness and the "critical government purpose."[443] The terms of the MOA did not require PSS to have warrants to zoom in on the WAMI for tracking and analysis; however, it did limit such actions to only when select felonious reports were made. The inability to positively identify any individual from the WAMI alone was reasonable to the majority. The AIR program was less intrusive than the approximately eight hundred mounted ground-level cameras through the CitiWatch program. Judge Bennett held that the majority refrained from applying *Carpenter* because it explicitly upheld "conventional surveillance techniques and tools, such as security cameras."[444] The ground-based cameras were viewed as more invasive because they "Often [employ] facial recognition software… allowing the police to immediately conclude who someone is and what they look like."[445] The majority concluded the section by emphasizing the limits applied to the AIR program to investigate individuals needing to meet probable cause and warrant requirements.

The panel next addressed the claim that the AIR program violated the freedom of association. The plaintiffs did not develop the argument or specify if the intimate association or expressive association right would be violated.[446] In the nature of a TRO, the panel rejected the likelihood of success on the merits. The implied claim that people have a right not to be seen in public places, of which the plaintiffs did not cite any precedent or doctrine, was also rejected. The panel concluded its decision by analyzing Baltimore's interest in using the AIR program in a

[443] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 18.
[444] *Carpenter v. United States*, 138 S. Ct. 2220 (2018)
[445] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 18-19.
[446] *Roberts v. U.S. Jaycees*, 468 U.S. 609, 619 (1984)

way that "serves the public interest."[447] In the spirit of *Jones*, the panel believed "elected officials should play a leading role in crafting policies that balance the need for public safety and the need for privacy."[448] They did not neglect the more contentious 2016 pilot program, which was not conducted with the consent or oversight of elected officials. In the 2020 version of the AIR program, "Constituents were heard and the BPD's contract with PSS was approved by elected officials with modified and substantially less intrusive conditions."[449] The majority opinion concluded by highlighting the number of murders in 2019 to demonstrate the legitimate public interest in accepting the experimental program. It is part of the primary duties of a government to provide for the "mutual preservation of [the people's] lives, liberties, and estates."[450]

Chief Judge Roger Gregory's dissent argued that *Carpenter* was the controlling case concerning the AIR program, not *Knotts* or the Flyover cases, as the majority argued. Chief Judge Gregory all but invoked the Mosaic Theory without stating it or referencing *Jones*, where the Supreme Court rejected the DC Circuit's embrace of it. Justice Sotomayor's concurring opinion in *Jones* was the closest any member of the Supreme Court has come to accepting the Mosaic Theory. Chief Judge Gregory built his dissent on an excerpt from *Carpenter's* majority opinion saying, "the Government could, in combination with other information, deduce a detailed log of Carpenter's movements." This passage could sound like an embrace of the Mosaic Theory, but nowhere else in the majority opinion is the statement developed. Instead, Chief Roberts relies on the "unique nature of cell phone location information" to explain the majority's warrant requirement for more than six days of individual location data in *Carpenter*.

Chief Judge Gregory vigorously contested the anonymity of those surveilled under the AIR program, again relying on Mosaic Theory reasoning in which one could identify common

[447] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 21.
[448] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 22.
[449] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 22.
[450] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 23, citing John Locke, Second Treatise on Government 178 (Mark Goldie ed., 1993) (1689).

patterns of life to obtain a positive identification of an individual surveilled. At no point in his dissent does he address the probable cause or warrant-satisfying requirements necessary for analysts to fuse the AIR collection with the Citiwatch footage or the law enforcement databases. By analyzing the AIR program without its in-built constraints, Chief Judge Gregory believed *Knotts* was violated, that "if "dragnet type law enforcement practices ... should eventually occur," then "different constitutional principles may be applicable." To Chief Judge Gregory, because the AIR program was the fusion of the WAPS, CitiWatch, law enforcement facial recognition software and databases, it was the dragnet *Knotts* cautioned against. The "different constitutional principle" that should be applied is the nonspecific Mosaic Theory. Chief Judge Gregory went further with *Carpenter*,

> A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U. S., at 351–352. A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones*, 565 U. S., at 430 (ALITO, J., concurring in judgment); id., at 415 (SOTOMAYOR, J., concurring).

Chief Judge Gregory cited Justice Alito's *Jones* concurrence, where the reasonable expectation of privacy was what the reasonable person would expect the government to do.[451] Chief Judge Gregory surmised the reasonable person would likely expect the CitiWatch camera to collect their movements but would not expect it to "secretly monitor and catalog every single movement of an individual's car for a very long period." Therefore, the AIR program was more invasive than ground-based surveillance. The totality of what could be revealed by the full analysis of a person of interest would undoubtedly reveal "the privacies of life"[452] or an "intimate window into a person's life."[453]

---

[451] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 327 (2012), https://ssrn.com/abstract=2032821

[452] *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1961) footnote; *Riley v. California*, 573 U.S. 373, 403 (2014)

[453] *United States v. Jones*, 565 U.S. 415 (2012) (Sotomayor concurring)

The concerns over protecting the "privacies of life" were the focus of Justice Sotomayor in her *Jones* concurrence. Even though AIR was limited to outdoor collection, the residents' subjective expectation of privacy in their day-to-day movements should be protected. Chief Judge Gregory believed the AIR program was more intrusive than *Knotts*. In *Knotts*, the police were limited to real-time tracking, but because of the forensic nature of the AIR program and the arbitrary limit of 45 days of data, there were no technical limits on what the AIR program could or could not collect. Thus any person in Baltimore could be tracked in detail "every moment of every day."[454] Chief Judge Gregory argued that "long-term, recorded surveillance of public movements uncovers… a person's most intimate associations and activities," as did *Carpenter's* timestamped CSLI data points.

Chief Judge Gregory explicitly rejected the majority's emphasis on the 12-hour nighttime collection gap and the anonymous identity of those who entered buildings. This mode of analysis by the majority followed a sequential approach: "these conclusions only hold up when limiting the Fourth Amendment analysis of the AIR program to solely the photographic data its planes collect."[455] Chief Judge Gregory emphasized what could be "deduced" "in combination with other information," citing Carpenter's CSLI analysis. Those phrases from *Carpenter* originated from *Kyllo*, where the "inference" from the outside information related to activities within a residence. Chief Judge Gregory was concerned with the potential to enable police to "deduce a comprehensive record of people's past movements" regardless if a warrant was required to access the information, a line further than Carpenter.[456] Under Carpenter, a warrant can grant law enforcement access to forty-five days of CSLI data. *Carpenter*, *Kyllo*, and *Knotts* all addressed the use of compiled warrantless data.

[454] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 30.
[455] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 32.
[456] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 33.

Chief Judge Gregory countered the majority's claim of anonymity of those surveilled, citing a 2013 study published in Scientific Reports. In "Unique in the Crowd," Montjoye and associates found "the uniqueness of human mobility traces is high and that mobility datasets are likely to be re-identifiable using information only on a few outside locations."[457] Chief Judge Gregory emphasized the finding that "Four randomly chosen points are enough to uniquely characterize 95% of the users." Chief Judge Gregory argued from this assessment that "when reviewing data showing a group of people's collective movements, an individual's movements tend to be so unique that it is not difficult to distinguish among people in the group."[458]

Chief Judge Gregory's assessment of the article's conclusion claimed too much. The study was based on 6500 antennas setup across a "small European country," tracing 1.5 million people for 15 months. They recorded approximately 114 interactions per month. The random spatiotemporal data points are vital to identifying unique characters. "This makes our random choices of points likely to pick the user's top locations (typically ''home'' and ''office'')."[459] The data samples uniquely identified where individuals spent most of their time. This function works well for mobile phone-based location tracking but is inapplicable to WAPS. When an individual remains static under GPS or CSLI tracking, the kind of data detectable by antennas, the data points populate at those static locations. Under aerial surveillance, the platform could not identify or track individuals inside structures; the quantity of data points would be significantly diminished. WAPS tracks changes over time. It can only identify points or persons of interest of those outside of structures with a clear line of sight to the aircraft.[460] If WAPS could see the

[457] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, & Vincent Blondel, "Unique in the Crowd: The Privacy Bounds of Human Mobility," Scientific Reports 3, 1376; 2, DOI:10.1038/srep01376 (2013).
[458] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 35.
[459] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, & Vincent Blondel, "Unique in the Crowd: The Privacy Bounds of Human Mobility," Scientific Reports 3, 1376; 4, DOI:10.1038/srep01376 (2013).
[460] WAPS with a resolution of one pixel per person cannot maintain a continuous identification of individuals if they are in a crowd or move under clouds, trees, or other natural environmental features that obstruct the image.

interior of structures, the data points would continue to populate. It would also trigger a simultaneous violation of *Kyllo*. The movement must be active to track a person or vehicle with WAPS. Once again, per the MOA, analysis of the data could not begin unless a request, probable cause, was established to analyze the data.

Chief Judge Gregory blurred the sequence of events, particularly between the data collection and analysis stages, because his analysis was based on a Mosaic Theory model. In addition, for CSLI or GPS data to be collected, the identity of the person or at least the device's metadata must be known before the query. A specific person is already being targeted. Chief Judge Gregory's argument would more accurately compare to geofencing. Geofencing is the practice of selecting a specific area, a digital fence if you will, and gathering the active cellular phone signals operating in that space. The metadata collected from geofencing is then processed and analyzed. Even with warrants, geofencing is still questionable under the individualized suspicion requirements.[461] Chief Judge Gregory's reliance on a Mosaic Theory approach was reinforced by criticizing the AIR program's integration with the Citiwatch camera network and the ALPR distributed throughout the city. The complaint refrained from challenging those networks, but the Chief Judge aggregated them in his analysis. In these criticisms, Chief Judge Gregory made clear that the objection to the AIR program was in its warranted capacity, not the operations of its warrantless capacity. The difference between data collected and analyzed is between reasonable, unwarranted, and reasonable, warranted searches. Until one can claim a right of privacy in public spaces, warrantless aerial surveillance is protected under the Flyover cases.

[461] *United States v. Chatrie*, 2022 U.S. Dist. LEXIS 38227, __ F.Supp.3d __, 2022 WL 628905 (United States District Court for the Eastern District of Virginia, Richmond Division March 3, 2022, Filed). https://advance-lexis-com.ccl.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:64XB-BYK1-JBT7-X0MM-00000-00&context=1516831.; Denise Lavoie, 'Geofence warrant' unconstitutional, judge rules in Virginia, Associated Press News, March 30, 2022, https://apnews.com/article/virginia-robbery-d20d767fa1ef52a8b69e76adb8626837 accessed October 7, 2022.

Chief Judge Gregory contested the applicability of the Flyover cases by the majority. In the Flyover cases, the Court permitted aircraft to fly over the locations of interest. The persistent loitering of an aircraft for up to twelve continuous hours, seven days a week, was a difference in kind.[462] The kind that "gives police access to a category of information otherwise unknowable."[463] This was *Jones's* essential question, which the majority did not address. The dissent of the Chief Judge channeled Justice Sotomayor's *Jones* concurrence concerning the revelation of the privacies of life, which made WAPS differences from CSLI or GPS data "inconsequential."[464]

Chief Judge Gregory rejected the majority's description of the AIR program as a Programmatic Search via *Carpenter* and the Mosaic Theory. As previously mentioned, Programmatic Searches are for "exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable"[465] When the Court upheld immigration and DUI checkpoints, the vehicle stops were recognized as "seizures"; however, the "measure of the intrusion" was "slight" when balanced with the state's interest in enforcing impaired driving or illegal immigration.[466] Chief Judge Gregory paralleled the AIR flight path with "roving patrols" deemed unreasonable in *Almeida-Sanchez v. United States*.[467] In *Almeida-Sanchez,* the Court upheld permanent and temporary checkpoints, not roving patrols who stopped and searched vehicles without probable cause or warrants.[468] The AIR program recorded its collection, the determining factor that made it transgressive of the Fourth Amendment.

---

[462] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 39.
[463] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 40 citing *Carpenter v. United States*, 138 S. Ct. 2218 (2018)
[464] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 40.
[465] *New Jersey v. T.L.O.*, 469 U.S. 351 (1985)
[466] *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990)
[467] *Almeida-Sanchez v. United States*, 413 U.S. 266 (1973)
[468] *Almeida-Sanchez v. United States*, 413 U.S. 266, 268 (1973)

Chief Judge Gregory disputed the majority's differentiation when the AIR program was "not being used to target particular individuals" and when it targeted particular individuals. This is because Chief Judge Gregory disregarded the difference between the collection and analysis stages of the AIR program. The majority applied the sequential approach of Fourth Amendment analysis wherein such distinctions were crucial to evaluating the reasonableness of government actions. The majority analyzed the dual function of the AIR program in its "slight" intrusion versus the reasonableness of a search upon the establishment of probable cause. The AIR program could not identify any individual before the probable cause was established, a bedrock of law enforcement investigative procedure.

Chief Judge Gregory did not distinguish aerial surveillance from CSLI data as distinct kinds of information; a categorical error was made by paralleling these two types of data, which could be used for similar purposes. Therefore, when Chief Judge Gregory cited *Carpenter*'s emphasis that the search occurred "when the Government accessed CSLI from the wireless carriers" as the reason why the AIR program should also be analyzed in the same way, it attempted to prove the argument from the negative. *Carpenter* did not include a discussion concerning the different stages of the PED process to prompt a discussion about the distinct stages of accessing, collecting, or analyzing information.[469] In *Carpenter*, the focus was if the Third Party doctrine should extend to CSLI data, which the United States assumed it had, if not for the "unique nature of cell phone location records"[470] With the focus on the possession of the data, how the data was used was secondary. In *LBS*, the primary question rested on what the BPD did with data.

Chief Judge Gregory concluded the analysis of WAPS by challenging the "special need" necessary to justify the AIR program as a Programmatic Search. Chief Judge Gregory applied

[469] PED is short for Processing, Exploitation, and Dissemination used in the Intelligence Community to describe stages of information handling.
[470] *Carpenter v. United States*, 138 S. Ct. 2217 (2018)

City of Indianapolis v. Edmond to make the argument.[471] Indianapolis set up temporary vehicle checkpoints for narcotics enforcement. Signage was posted along the road announcing the checkpoints, which directed drivers to prepare to stop and present identification and vehicle registration. The officers conducted an "open-view examination of the vehicle from the outside" and looking for visual signs of impaired occupants.[472] A drug detection dog would also walk around the vehicle. The Court denied the checkpoints as unreasonable seizures violating the Fourth Amendment. To overcome the individualized suspicion of wrongdoing requirement,[473] Indianapolis had to establish a special need to justify the Fourth Amendment seizure of the vehicles and persons being stopped. Instead, the court found the checkpoints pursuant to "ordinary criminal wrongdoing."[474] Chief Judge Gregory argued the AIR program's role in stopping violent crime was not a "special need" but instead a "paradigmatic example of "the normal need for law enforcement."[475] *Edmond* clarified, "there are circumstances that may justify a law enforcement checkpoint where the primary purpose would otherwise, but for some emergency, relate to ordinary crime control."[476] The Special Needs cases cited in *LBS* concerned temporary, indiscriminate, suspicionless seizures. Stopping people or vehicles absent individual suspicion of a crime were uncontested Fourth Amendment seizures. The harm caused by such actions was facially apparent. The harm caused by the AIR program was not so obvious, especially if one applied a sequential approach to the analysis instead of a Mosaic Theory. No seizure had taken place. The reasonableness of the search relied on the interpretive model applied.

The remaining sections of the dissent addressed factors specific to the TRO, a broader criticism of policing in Baltimore, and its disparate impact on the Black community. According to

---

[471] *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000)
[472] *City of Indianapolis v. Edmond*, 531 U.S. 35 (2000)
[473] *City of Indianapolis v. Edmond*, 531 U.S. 37 (2000)
[474] *City of Indianapolis v. Edmond*, 531 U.S. 41 (2000)
[475] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 44.
[476] *City of Indianapolis v. Edmond*, 531 U.S. 44 (2000)

Fourth Circuit precedent, the irreparable harm to Leaders of a Beautiful Struggle was the violation of the Fourth Amendment via WAPS.[477] In *New York Times v. Sullivan*, "The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." Whether or not the Fourth Amendment is protected as much as the First Amendment is a different research question. The critique of BPD was supported by a 2016 DOJ report which cataloged a "widespread pattern" of officers detaining people without reasonable suspicion. Those detainments "produce severe and unjustified disparities in the rates of stops... of African Americans " and "uncover[ed] evidence of criminal activity" at an "extremely low rate."[478] The DOJ report led to a federal consent decree in 2017.[479] A 2020 survey by Morgan State University in accordance with the consent decree, reported the majority of Baltimore residents personally witnessed racially discriminatory behavior by BPD.[480] Under this shadow of past behavior, skepticism against innovative technologies by judges and the community are more than reasonable.

In the en banc panel, Chief Judge Gregory wrote the majority opinion. The detailed analysis of Chief Judge Gregory's dissent in the three-judge panel thus became the majority opinion. The BPD did not petition the Supreme Court. The AIR program in the jurisdiction of the Fourth Circuit cannot operate. The ruling does not necessarily mean WAPS cannot operate in the jurisdiction in any form. For a new WAPS program to operate, the facts must be sufficiently different to warrant a new case or controversy. For example, if the WAPS system was not integrated into the same systems as the AIR program, it might survive scrutiny under the en banc panel's judgment. At the time of the en banc panel, archived AIR data was used in two

[477] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 44. Citing *Ross v. Meese*, 818 F.2d 1132, 1134–35 (4th Cir. 1987)
[478] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 46-47.
[479] Consent Decree, Baltimore Police Department, https://www.baltimorepolice.org/transparency/consent-decree-basics/consent-decree accessed October 11, 2022.
[480] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2020), 46-47.

hundred cases.[481] The constitutionality of WAPS by this panel did not introduce new arguments from the three-judge panel. The majority relied on mosaic theories suggested in the *Jones* concurrences by Justices Alito and Sotomayor and applied *Carpenter*.

In a separate concurrence, Chief Judge Gregory, with three others from the panel, questioned the role of policing in violence prevention at large. “Policing ameliorates violence, and restraining police authority exacerbates it. As surely as water is wet, as where there is smoke there is fire, the dissent takes for granted that policing is the antidote to killing.” The concurrence challenged the dissent’s lack of attention to the systemic factors contributing to the high crime rates, “Despite passing references to “systemic inequality,” “interrelationships,” and “foundational ill[s],” the dissent entirely disregards the systems, relationships, and foundational problems that have perpetuated Baltimore’s epidemic of violence.”[482] The systems of inequality formally segregating blocks by race had since lead to disparities to include, “investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates; and the list goes on.”[483] The link between those systemic inequalities and the AIR program were exemplified in the 2017 budget with greater proportional funding to policing versus “education, transportation, and housing combined.”[484]

The dissent of the en banc panel criticized the majority’s opinion on five points. Three focused on the procedures of the case. Two, the role of states within the federalist structure and how cities respond to violent crime were applicable to the policy decisions surrounding WAPS.

---

[481] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2021) (en banc), 9.
[482] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2021) (en banc), 33-34.
[483] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2021) (en banc), 34.
[484] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2021) (en banc), 35.

Baltimore has long struggled with violent crime, homicides included. The dissent highlighted that in 2017 Baltimore had more murders than New York City, with 1/14th the population.[485] They were critical of the majority's concern of "oversurveillance" above the danger of violent crime. The AIR program was a temporary, six-month pilot program that sought to innovate a new means of combating violent crime. The program actively consulted the concerns of the communities and retained civil rights experts for the duration of the program. Despite the good faith efforts of the city, the majority saw it appropriate to prohibit the attempt. Were it not for the court's dawdling, the WAPS would not have had the opportunity to operate at all. This laboratory of democracy failed the institutional review board in the eyes of the majority.

> "In its indecorous rush to quash any experimentation on Baltimore's part, the majority has signaled to American cities that future initiatives and attempts at solving the rapid rise of violent crime will likely meet with disfavor from the courts… Its decision strikes a heavy blow against democratic experimentation and innovation that is essential if our nation is to make headway in protecting those most vulnerable to the ravages of crime… No one claims that police departments are without their blemishes, or that history is without its stains, or that reforms themselves are without their problems and complexities… But the question before us is, again, whether the people shall be left a proper latitude to address those problems or whether courts will presume to decide what is best for them."[486]

Had the majority evaluated the other pre-existing surveillance programs integrated into the AIR program under the same Fourth Amendment interpretation, they likely would not have survived the Court's broad application of *Carpenter*. Nevertheless, the CitiWatch network continues to be in use as they have been since 2005.[487]

Chapter 7

WAPS May Be Constitutional

---

[485] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2021) (en banc), 41.
[486] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495 (4th Cir. 2021) (en banc), 43-44.
[487] Maryland General Assembly Office of Legislative Audits, Baltimore Police Department Performance Audit Surveillance Equipment, 11, Baltimore, 2022, accessed October 13, 2022, https://dls.maryland.gov/pubs/prod/NoPblTabPDF/BPD-Surveillance22.pdf

LBS is not a perfect case to evaluate the constitutionality of WAPS. The Courts did not evaluate WAPS in isolation between the integrated structure of the AIR program, the specific conditions of the MOA, and the TRO at the center. This chapter will address those factors, suggest the operating conditions in which other localities may constitutionally operate WAPS, and consider the implications of privately used WAPS.

The bright line test to the constitutionality of WAPS should be whether PII is revealed or not. This line is sufficient for any emerging technology. PII is the dividing line between the general public and a specific person. It is not a new standard of information for government stewardship when differentiating between public and private information. PII is the line for one's reasonable expectation of privacy; it also fits Justice Alito's definition because Congress has already defined it as information the public would expect to be secured. PII is a well-established definition. It has been used in government operations since 1994, thus making it a pragmatic line one need not need a graduate degree to understand.[488]

The protection of PII is the superior line of demarcation over any of the other models of Fourth Amendment interpretation to calculate whether WAPS or any other emerging technology has violated a reasonable expectation of privacy. The probable cause and warrant requirements should apply if an individual's PII is discoverable. This line is more practical than the Proportionality Principle of Slobogin, the Quantitative Right to Privacy of Citron & Gray, or the Collective Right to Privacy of Gray. It is more articulable than the differentiation between tools, systems, or units of surveillance, as Ferguson suggested. The evaluation of PII follows the sequential approach to Fourth Amendment interpretation observed by Kerr. It thus does not require a paradigm shift of constitutional interpretation to identify if and how WAPS might be

[488] 18 U.S.C.A. § 2725 (3), "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.," 108 STAT. 2102 Public Law 103-322—Sept. 13, 1994

constitutionally operated. A reliance on PII would fit well within Kerr's equilibrium adjustment model.

Slobogin, Citron, and Gray each suggested new Fourth Amendment interpretations, which were, in some form, a Mosaic Theory. The more generalized definition of a Mosaic Theory is an analysis based on the aggregated information to be determined post hoc of an investigation or operation. Thus, unless the investigating bodies can accurately prophesy the violations and perpetrators, they would have to risk entire investigations being found inadmissible after the fact. The definition alone makes it impractical for any law enforcement agency to determine how investigations should be conducted if the purpose is to gather admissible evidence for a criminal conviction. Law enforcement would be effectively bound by the investigative techniques developed in the previous century. They would be banned if not significantly disincentivized to innovate new methods of investigation with the ever-growing tools and technologies of the present age. Any court that adopts a Mosaic Theory of the Fourth Amendment will likely reject WAPS as a potential constitutional surveillance technology.

Slobogin's Proportionality Principle was more workable than the Mosaic Theory presented in *Jones* and *Maynard*, but its reliance on ex ante review made it a nonstarter on practical grounds. When the Court considers overturning precedent, the reliance interests are often a significant factor. Reliance interests refer to the effects of a particular ruling or decision.[489] Often when major legal doctrines are challenged, the reliance interests contribute to the court's determination if the problematic portion is severable from the law at issue. For example, the main question in *California v. Texas*, a 2020 attempt to overturn the Affordable Care Act, the question before the court was if the taxing clause was severable from the rest of the law. If it were, then the ACA would have remained. If it were not, the entire law would have

[489] Gary Bridgens, "Demystifying Reliance Interests in Judicial Review of Regulatory Change," George 29 Mason Law Review 1, 2021, accessed September 21, 2022, https://lawreview.gmu.edu/print__issues/demystifying-reliance-interests-in-judicial-review-of-regulatory-change/

been overturned.[490] The reliance interests challenged by a paradigm shift in Fourth Amendment jurisprudence are among the problems implementing the Mosaic Theory. Kerr described the difficulty, "implementing it would require the creation of a new set of Fourth Amendment rules-in effect, a mosaic parallel to the sequential precedents that exist today."[491] The Proportionality Principle answered some of the questions required of a knowable theory but not enough to be a workable theory.

Gray and Citron's Right to Quantitative Privacy shifted the focus of the Mosaic Theory from "how much" information was gathered to "how" information was gathered to determine if the method conflicted with the Fourth Amendment or not. They admitted that the Mosaic Theory was not facially compatible with the Plain View or Third Party doctrines.[492] Their model was designed to focus on multi-sourced databases, such as New York's Domain Awareness System, which compiled and data mined "video streams from 3,000 public and private security cameras, images from license plate readers and traffic cameras, and data from government and private databases."[493] Their Quantitative Right of Privacy approach would determine "whether an investigative technique or technology has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government."[494] Their model solved half of the Mosaic Theory's difficulty by resolving some conflicts with the Third Party doctrine.[495]

---

[490] *California v. Texas*, 593 U.S. ___ (2020)
[491] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 346 (2012), https://ssrn.com/abstract=2032821
[492] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review 62 (2013), 68, https://scholarship.law.umn.edu/mlr/285
[493] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review 62 (2013), 66, https://scholarship.law.umn.edu/mlr/285
[494] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review 62 (2013), 101, https://scholarship.law.umn.edu/mlr/285
[495] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review 62 (2013), 141, https://scholarship.law.umn.edu/mlr/285

However, that is only half the problem. Adoption of the Mosaic Theory would require the Court to overturn *Knotts*.[496]

Quantitative privacy approached the issue from a technological standpoint. They argued that *Knotts* and *Jones* were different because of the differences between short-range radio beacons and satellite GPS trackers. The emphasis on the capabilities of the technology might have appeared to resolve the concern between the specific facts of *Knotts* versus *Jones*. However, Kerr pointed out that the second difficulty of administering the Mosaic Theory, in this example it applied, was the "rapid pace of technological change."[497] WAPS was a novel technology that was neither a GPS tracker nor a radio beacon. The technology-centered approach fell short. WAPS is imagery intelligence; *Knotts* and *Jones* relied upon signals intelligence, a significant categorical difference. Signals intelligence is based on known electronic signals such as radio frequencies, cellular metadata, or other electromagnetic waves on the spectrum. Signals-based surveillance starts with an identified party to track and trace, the sort that would qualify as PII. Imagery intelligence is based on whatever is publicly viewable, and additional analytical steps must be made to ascertain identifying information. Thus, PII is not known. The technology-centered focus of the Quantitative approach to privacy would permit only "conventional surveillance techniques and tools," to which the *Carpenter* court was cautious that "we do not "embarrass the future," expressing the narrow scope of the opinion.[498] Gray and Citron's model would not permit WAPS under any circumstances because of broad potential for "indiscriminate surveillance."

[496] David Gray and Danielle Citron, "The Right to Quantitative Privacy," 98 Minnesota Law Review 62 (2013), 132, https://scholarship.law.umn.edu/mlr/285
[497] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 311, 347 (2012), https://repository.law.umich.edu/mlr/vol111/iss3/1
[498] *Carpenter v. United States*, 585 U.S. 2220 (2018)

Gray and Citron represent the most adapted legal model in the spirit of Neil Richard's Information Privacy Law Project.[499] The Project's goal has been to encourage Information Privacy, which is "the right of individuals to control information about themselves." Much of the scholarship amongst Information Privacy scholars belongs to what is now described as Surveillance Studies. Richard's article was a long book review of Daniel Solove's "The Digital Person: Privacy and Technology in the Information Age" where the concern was the way "law and legal theory approach the social, political, and legal implications of the collection and use of personal information in computer databases."[500] Solove and Richards' concerns were focused on aggregating digital information, regardless if the information was aggregated or held by public or private organizations. Solove sought to describe the problems of privacy information in systemic or architectural rather than individualized terms.[501] Of the same school of thought, Shoshanna Zuboff's 2019 "The Age of Surveillance Capitalism" echoed similar concerns with extensive details of how Big Data collects and analyzes information about every individual who uses their products.[502] Solove and Zuboff's theories would certainly be concerned with WAPS, regardless if it were in public or private control. However, their frameworks were much broader and more generalized than constitutional jurisprudence. The premise of such Surveillance Studies rejects the principles behind constitutional interpretation to apply to the questions of this research.

---

[499] Neil M. Richards, "The Information Privacy Law Project," 94 Georgetown Law Journal (2006) Washington University School of Law Working Paper No. 06-11-01, https://ssrn.com/abstract=941181, 1087.
[500] Neil M. Richards, "The Information Privacy Law Project," 94 Georgetown Law Journal (2006), Washington University School of Law Working Paper No. 06-11-01, https://ssrn.com/abstract=941181, 1090.
[501] Neil M. Richards, "The Information Privacy Law Project," 94 Georgetown Law Journal (2006) Washington University School of Law Working Paper No. 06-11-01, https://ssrn.com/abstract=941181, 1095.
[502] Shoshanna Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Public Affairs, 2019.

Ferguson's approach to WAPS was the newest adaptation of a Mosaic Theory. It developed further aspects of the quantitative privacy approach by separating persistent surveillance from conventional surveillance. Ferguson found this space to develop in existing precedent via *Riley v. California*, in which the Court recognized the sensitivity of warrantless searches of a cellular phone's contents. The cell phone was removed from Riley, incident to an arrest, for safety reasons. The Court found no justifiable connection to searching the phone's contents for safety purposes. The injury was the extent of information held on the device. The removal of the phone was not a violation; the search/analysis of it was, under the PII model, the result would have been the same as the unanimous opinion. Ferguson used this case to argue for the Court's implicit agreement with his approach.[503] It was bold to build new legal approaches from implied statements from the court. Using implied text from Court opinions was how Chief Judge Gregory viewed *LBS* as a Mosaic Theory embracing case. The practice of judicial restraint tends to lead the Court to make more minor incremental changes instead of decisive decisions.[504] Ferguson's dividing line between analog versus digital technology runs against Kerr's decade-old criticism.[505] Technology continues to develop at too rapid a pace to base a legal framework around it. Doing so would effectively cut off the available technologies at the time of the rulemaking. This approach would be satisfactory if the intent were to cease new technologies' development and innovation. As the litmus test, PII remains the best approach that can be applied to new technologies without hindering the continued development of new technologies.

Because PII is the most reasonable approach within the current jurisprudence as the Supreme Court has defined, bright lines should be drawn to articulate when WAPS might cross

---

[503] Andrew Guthrie Ferguson, "Persistent Surveillance," Alabama Law Review, Forthcoming, 23, https://ssrn.com/abstract=4071189

[504] *Dobbs v. Jackson Women's Health Organization*, No. 19-1392, 597 U.S. ___ (2022), slip op. at 137

[505] Orin Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Michigan Law Review 346 (2012), https://ssrn.com/abstract=2032821

the line between public view data and personal identifying information. Unlike signals intelligence, imagery intelligence is inherently more limited to identifying individuals. The Memorandum of Agreement in the AIR program had extensive conditions specific to Baltimore for the WAPS operation. This next section will evaluate the limitations of the MOA under the PII test and discuss where the conditions could have been more or less restrictive and remain constitutional under the equilibrium adjustment model of Fourth Amendment analysis.

The AIR program was fielded as a six-month pilot program based on the available funds from Arnold Ventures, a criminal justice-focused philanthropy.[506] Presumably, future long-term WAPS programs considered by state or local governments would be taxpayer funded for the purpose but not limited to assisting law enforcement. The Urban Institute estimated that in 2019, state and local governments spent 3.7% of their budget on police, of which 97% were salaries and benefits.[507] The costs of WAPS are considerable. The MOA requested about 3.7 million dollars to operate from March to December 2020.[508] This was for three WAPS-equipped aircraft and over thirty personnel who, based on the per diems, were not local to Baltimore. However, WAPS is likely more cost-effective than law enforcement helicopters. In 2020, Los Angeles County Sheriff's Department spent 23 million dollars on helicopter maintenance alone.[509] The primary critique of current law enforcement aerial surveillance is the limited view. Even with high-resolution, GPS-integrated night vision cameras, they have still been limited by the soda

[506] Michael S. Harrison, "Professional Service Agreement Acceptance," Baltimore Police Department, March 17, 2020, 1, accessed June 16, 2022 https://www.baltimorepolice.org/sites/default/files/General%20Website%20PDFs/MOU_AIR_Presented_to_Board_of_Estimates-compressed.pdf

[507] "Project State and Local Backgrounders: Criminal Justice Expenditures: Police, Corrections, and Courts," Urban Institute, accessed October 17, 2022, https://www.urban.org/policy-centers/cross-center-initiatives/state-and-local-finance-initiative/state-and-local-backgrounders/criminal-justice-police-corrections-courts-expenditures

[508] Michael S. Harrison, "Professional Service Agreement Acceptance," Baltimore Police Department, March 17, 2020, 26-27, accessed June 16, 2022

[509] "Sheriff Villanueva Announces LASD Budget Underfunded by $400 Million," Los Angeles County Sheriff's Department, May 4, 2020, accessed October 15, 2022, https://lasd.org/lasd-budget-underfunded-by-400-million/

straw effect.[510] A single WAPS system could potentially replace several helicopters, leading to reduced equipment and maintenance costs and lower fuel consumption, thus fewer emissions and costs. WAPS aircraft can have preselected flight routes or adjust for particular emergencies without alerting fleeing suspects to respond with more dangerous behaviors, such as high-speed pursuits, which can lead to injuries and property damage.[511] These safety, fiscal, and environmental benefits are some of the many benefits why WAPS systems would be superior to the widely used law enforcement helicopters.

Gregory McNeal, a law professor at Pepperdine's Caruso School of Law, is one of the leading scholars on drone policy and regulation. McNeal provided core recommendations to legislators for drone usage per the Flyover Cases.[512] McNeal analysis adhered to a sequential approach to the Fourth Amendment. Several of McNeal's core drone use and data storage recommendations were applicable to WAPS. It is important to note that the recommendations were for legislators to make laws regarding drone use, specifically by government actors. Ultimately, in a representative government, legislators should be the ones to make these determinations, not courts. Justice Alito noted as much in his *Jones* concurrence.[513] The specific aspects of WAPS collection legislators should determine are duration, frequency/time, resolution, integration, accessibility, and limitations. With each of these factors, I will analyze the conditions of the AIR program and whether they were optimized within a constitutional understanding. For the sake of analysis specific to WAPS, it will not consider other surveillance tools beyond public information and archived data databases.

---

[510] Kim Zetter, "NYPD Helicopter Views Faces from Miles Away," Wired Magazine, last modified June 5, 2008, accessed July 21, 2021, https://www.wired.com/2008/06/nypd-helicopter/

[511] California Highway Patrol, "Report to the Legislature SB719," State of California, November 2021, accessed February 10, 2023, https://www.chp.ca.gov/Documents/2021%20SB%20719%20-%20Police%20Pursuits.pdf

[512] Gregory S. McNeal, "Drones and Aerial Surveillance: Considerations for Legislators," (November 11, 2014), Brookings Institution: *The Robots Are Coming: The Project on Civilian Robotics*, November 2014, Pepperdine University Legal Studies Research Paper No. 2015/3, accessed April 2, 2019, https://ssrn.com/abstract=2523041

[513] *United States v. Jones*, 565 U.S. 400, 427-428 (2012).

How long can a WAMI system operate to be considered “persistent” without violating *Carpenter*, *Knotts*, or *Karo*? This is not ceding the argument that these cases apply to WAPS, but to demonstrate whether the AIR program accurately assessed violated any of these cases. *Carpenter* found persistent CSLI location information for more than six days of data constituted an unreasonable search.[514] *Knotts* ruled that three days of intermittent radio signals were not an unreasonable search.[515] *Karo* determined that two hundred twenty-two days of radio signals were not unreasonable. However, any time “in a private residence, a location not open to visual surveillance” with a “justifiable interest in the privacy of the residence” violated the Fourth Amendment.[516]

When the Court considered persistent surveillance in *Knotts* and *Karo*, the duration was secondary to the location of the tracking device. In *Carpenter*, the court emphasized the “unique” characteristics of CSLI twice. In the three Flyover cases, the record did not reflect more than a cursory flyover by the aircraft. Thus, the duration was not a consideration. The radio beacons and CSLI were actively relaying location information to the officers and the cellular phone provider. In *Riley* and *Carpenter*, when duration was considered, the persons of interest were known and thus were personally being searched.

Aerial surveillance is passive information gathering, meaning it does not prompt data creation; it collects what was passively available, information revealed to the public from “navigable airspaces.”[517] The “persistent” portion of WAPS referred to the duration the imagery sensors were operating. Per the MOA, the AIR program was limited to eight hours a day and prohibited from collecting during nighttime hours. These restrictions were not necessary under constitutional scrutiny. Even if a strict application of *Carpenter* was applied to WAPS, aircraft could continuously collect information for six days without interruption without a Mosaic Theory

[514] *Carpenter v. United States*, 585 U.S. 2202, 2013 (2018)
[515] *United States v. Knotts*, 460 U.S. 276, 279 (1983)
[516] *United States v. Karo*, 468 U.S. 705, 714 (1984)
[517] *California v. Ciraolo*, 476 U.S. 207, 213 (1986)

application. The duration of an appropriate interruption to be considered a break in the persistence should be defined by legislators. Mechanical limitations would likely lead to operational coverage gaps, as would data analysis to determine optimal hours of operation. However, such factors should not be the basis of the permissibility of the surveillance. Without the Mosaic Theory reading, persistence refers to the continuous collection, not what could be surmised. As a point of consideration, the US military's long-term goals for WAPS have been airships that could endure for multiple days or weeks.[518] This is not to say such systems would be permitted for domestic use, but WAPS began as military technology for military applications. One must be aware of what might be sought for domestic applications in the future.

How detailed can the imagery be without violating *Dow Chemical* or *Kyllo*? In *Dow Chemical*, the Court was not persuaded by the advanced technology of the camera used to capture private property. "The [district] court emphasized that use of "the finest precision aerial camera available" permitted EPA to capture on film "a great deal more than the human eye could ever see."[519] The commercially available camera had the capability with "simple magnification" to identify objects as small as ½ inch diameter wires.[520] The Court was concerned the camera may have revealed "intimate details as to raise constitutional concerns," but it did not. "Intimate details" as defined by precedent looked to *Oliver v. United States*, the 1984 case which reaffirmed the Open Fields doctrine.[521] *Oliver* pointed to *Boyd*, which pointed to the 1765 English case of *Entick v. Carrington*, which sought to uphold "the sanctity of a man's home and the privacies of life."[522] Justice Sotomayor's *Jones* concurrence argued that GPS data could indicate visits to locations of a "private nature." The Court has not clearly extended

[518] Jen Judson, "The Airship Formerly Known as LEMV To Fly Again," DefenseNews, accessed October 15, 2022, https://www.defensenews.com/industry/2016/05/12/the-airship-formerly-known-as-lemv-to-fly-again/
[519] *Dow Chemical Co. v. United States*, 476 U.S. 227, 230 (1986)
[520] *Dow Chemical Co. v. United States*, 476 U.S. 227, 238 (1986)
[521] *Oliver v. United States*, 466 U.S. 170, 180 (1984)
[522] *Boyd v. United States*, 116 U.S. 616, 630 (1886)

the understanding of “intimate details” beyond activities from inside one’s home. It is important to emphasize that such protections do not apply to mere private property. In each of the Flyover cases, private property was observed without issue.

Kyllo established two rules to apply to new technologies and Fourth Amendment searches, “We think that obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area,” constitutes a search… at least where (as here) the technology in question is not in *general public use*.”(emphasis added) Despite what the entertainment industry might portray, aerial thermal imagery does not (yet) see through structures. If it is developed, it would unquestionably require a warrant for domestic use based on the first part of *Kyllo*. The second part of *Kyllo* established the “general public use” rule, which has the most potential to limit the kinds of technology used in future WAPS systems. In footnote six of the *Kyllo* majority, Justice Scalia acknowledged the “potential uncertainty… by noting that whether or not the technology is in general public use” but declined to address that factor. At the operational level, as long as the probable cause must be established prior to any analysis of WAPS, the resolution capacity is moot. One would not know the benefits of higher-resolution technology until the analysis stage may commence. Once the probable cause has been established to allow the images' analysis, the images' clarity would not conflict with *Kyllo*. Compounding this point, the ARGUS-IS camera, with its 1.8 gigapixel resolution, almost ten times that of the Hawkeye II used in *LBS*, used the same photographic chips from iPhone 8 cameras.[523] The deployment of secret advanced military technology is not necessary. As mentioned earlier, the likelihood of state or local governments employing higher resolution cameras than Hawkeye II is fiscally limiting, but under this sequential analysis, not constitutionally limiting.

[523] Arthur Holland Michel, location 1591.

As it was in the AIR program, WAPS likely will be integrated with other surveillance systems when used by law enforcement. The Computer Aided Dispatch (CAD),[524] Shotspotter,[525] Citiwatch,[526] and ALPRs were preexisting tools integrated with WAPS in the AIR program. At the most basic level, future programs with WAPS would include CAD systems to identify events of interest. Additional emerging technologies and techniques such as facial recognition, geofencing, mobile x-rays, cell site simulators, and DNA databases might also be integrated into complex law enforcement systems. Each would likely be challenged in the courts. Suppose one maintains constitutional analysis with the sequential approach as long as each individual system is permissible. In that case, integrating and synchronizing multiple systems will not raise a Fourth Amendment objection. Much of the scholarship has focused on this concern and the heart of the Mosaic Theory. The PII standard is sufficient to analyze each of these technologies.

Facial recognition, geofencing, cell site simulators, and DNA databases should each require probable cause before deployment. They each rely on identifying known individuals or values for the collection to commence. Facial recognition attempts to match images of known individuals with images of unknown individuals. Its use in law enforcement has already been shown to be problematic due to the unconscious bias of programmers and samples for the algorithms lacking diversity.[527] Geofencing has already failed at the Fifth Circuit.[528] Cell site

---

[524] TechNote: Computer Aided Dispatch Systems, DHS Science and Technology, September 2011, accessed October 17, 2022, https://www.dhs.gov/sites/default/files/publications/CAD_TN_0911-508.pdf

[525] Shotspotter Inc., accessed October 17, 2022, https://www.shotspotter.com/precision-policing-platform-technology/

[526] CitiWatch Community Partnership Overview, Baltimore Police Department, accessed April 17, 2021, https://www.baltimorepolice.org/community/citiwatch-community-partnership-overview

[527] Joy Buolamwini, "Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers," (2017, MIT Master's Thesis) accessed June 18, 2020, https://www.media.mit.edu/publications/full-gender-shades-thesis-17/; Alex Najibi, Racial Discrimination in Face Recognition Technology, Harvard University Science in the News Blog, October 24, 2020, accessed October 18, 2022, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

[528] *United States v. Chatrie*, 2022 U.S. Dist. LEXIS 38227, __ F.Supp.3d __, 2022 WL 628905 (United States District Court for the Eastern District of Virginia, Richmond Division March 3, 2022, Filed). https://advance-lexis-com.ccl.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:64XB-

simulators are sensitive technology that state and local law enforcement use under the supervision of federal intelligence agencies.[529] In *Maryland v. King*, the court decisively found that taking a DNA sample was a search. “It can be agreed that using a buccal swab on the inner tissues of a person’s cheek in order to obtain DNA samples is a search.”[530] In *King*, DNA collected incident to an arrest was not protected from being used in DNA databases. Likewise, using DNA collected and held by ancestry organizations for law enforcement has led to significant arrests and constitutional questions. So far, such information falls under Third Party doctrine. The fact that familiar DNA has been used to identify perpetrators has complicated this issue.[531]

Shotspotter and tools like CitiWatch, ALPR, and mobile X-Ray vans operate on public view doctrine. Shotspotters are ground-based audio surveillance systems. Using state-of-the-art audio analysis with a network of microphones, they approximate the location of gunshots in the sensor coverage area. Shotspotters cannot identify individuals. They use acoustic wave technology to provide locations of gunfire. Citiwatch and other security cameras mounted throughout Baltimore and other locales were expressly protected in *Carpenter* as “conventional surveillance techniques and tools.”[532] ALPR photographs the license plates traveling on public roadways in view of the public. However, the probable cause should be established for ALPR to search the databases from the collected data. X-Ray vans using backscatter technology have

---

BYK1-JBT7-X0MM-00000-00&context=1516831.; Denise, Lavoie, ‘Geofence warrant’ unconstitutional, judge rules in Virginia, Associated Press News, March 30, 2022, https://apnews.com/article/virginia-robbery-d20d767fa1ef52a8b69e76adb8626837 accessed October 7, 2022.

[529] Cyrus Farivar, “Warrantless Stingray Case Finally Arrives Before Federal Appellate Judges,” Ars Technica, January 29, 2016, accessed October 18, 2022, https://arstechnica.com/tech-policy/2016/01/warrantless-stingray-case-finally-arrives-before-federal-appellate-judges/; Nicky Woolf, “2,000 Cases May Be Overturned Because Police Used Secret Stingray Surveillance” The Guardian, September 4, 2015, accessed October 18, 2022, https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance

[530] *Maryland v. King*, 569 U.S. 435, 446 (2013).

[531] Paige St. John, “The Untold Story of How the Golden State Killer was Found: A Covert Operation and Private DNA,” Los Angeles Times, December 8, 2020, accessed October 18, 2022, https://www.latimes.com/california/story/2020-12-08/man-in-the-window

[532] *Carpenter v. United States*, 585 U.S. 2202, 2220 (2018)

been used by NYPD along public roads since 2012.[533] The appellate division of the New York Supreme Court ruled that the routes and collection of those vans were not subject to Freedom of Information Law (FOIL) disclosures due to their sensitive nature. However, the NYPD was required to disclose the radiation reports from the potential harm caused by the scans. Due to the invasive nature of backscatter scans via *King*, this technology likely violates the Fourth Amendment under a sequential analysis from unsuspecting subjects who happen to drive or park near the vans.

It is important to emphasize that the analysis of these technologies described above has been focused on the collection stage. Probable cause ought to be established with every technology which processes the information. The processing would separate individuals from the public at large, thus prompting the individualized suspicion requirement of reasonable searches. When any of these tools or systems process the collected data, PII is identified or created.

The WAPS data should be accessible to the public. Just like data retention, access to the data should specifically be determined by legislators. McNeal suggested retention policies divided by 30, 90, and 120-day increments, from when law enforcement should have varying levels of access based on "immediate complaints," "reasonable suspicion," and "probable cause." The final increment is the destruction of the data.[534] I would go further and argue for public access to the WAPS data at the same levels as law enforcement access. Thus, 30 days of immediate collection should be accessible to the public, and 90 days after the collection, requests for information (RFI) should be able to be submitted to the WAPS administration. At this point, WAPS should not be monopolized by law enforcement.

---

[533] *Michael Grabell v. New York City Police Department*, Yale Law School Media Freedom and Information Access Clinic, accessed October 18, 2022, https://law.yale.edu/mfia/projects/government-accountability/michael-grabell-v-new-york-city-police-department

[534] Gregory S. McNeal, "Drones and Aerial Surveillance: Considerations for Legislators," Brookings Institution: The Robots Are Coming: The Project on Civilian Robotics, November 2014, Pepperdine University Legal Studies Research Paper No. 2015/3, https://ssrn.com/abstract=2523041

City and state governments should administer WAPS systems under an organization directly answerable to the people. In some locales, this may be a separate administrative agency; in others, WAPS might be under the Chamber of Commerce, the City Council, or a Joint Powers Agency.[535] This is twofold. First, WAPS has utility far beyond law enforcement purposes, the point that Ross McNutt has demonstrated.[536] Locals could use the data to trace traffic flow, monitor erosion control, vegetative density, and a host of other governmental or private interests in wide area imagery. Second, as a means to practice transparency to the public. One of the selling points of the AIR program to civil rights groups was the ability to exonerate wrongfully charged individuals, provide evidence for defense attorneys, and track police movement to calls for service.[537] The AIR program had no such examples of criminal defense assistance. To avoid potential conflicts of interest, WAPS should be maintained by non-law enforcement entities. Whether or not the administration could provide analysis of the WAPS data to public and private offices would depend on the legislature's interests. I would suggest sufficient funding provide imagery analysts who could analyze the data for criminal cases on an equal field, be the request for the prosecution or the defense, provided sufficient documentation to justify the search criteria by the analysis. The structural availability and disclosure of Brady material would provide the mechanism that such disclosures would not be the exception but the norm.[538] Commercial interests could be expected to pay reasonable service fees for the data

---

[535] Trish Cypher and Colin Grinnell, "Governments Working Together: A Citizen's Guide to Joint Powers Agreements," California State Legislature Senate Local Government Committee, accessed October 20, 2022, https://sgf.senate.ca.gov/sites/sgf.senate.ca.gov/files/GWTFinalversion2.pdf

[536] Ross McNutt, "Wide Area Surveillance in Support of Law Enforcement," Persistent Surveillance Systems, January 2014.

[537] Rosanna Smart, Andrew R. Morral, Terry L. Schell, "Evaluating Baltimore's Aerial Investigation Research Pilot Program," RAND Social and Economic Well-Being, Justice Policy Program. Santa Monica, CA, RAND Corporation, 2022, accessed June 6, 2022, https://www.rand.org/pubs/research_reports/RRA1131-2.html.
Andrew R. Morral, Terry L. Schell, Brandon Crosby, Rosanna Smart, Rose Kerber, and Justin Lee, "Preliminary Findings from the Aerial Investigation Research Pilot Program," Santa Monica, CA: RAND Corporation, 2021. Accessed May 9, 2021, https://www.rand.org/pubs/research_reports/RRA1131-1.html.

[538] "Brady Rule," Legal Information Institute Cornell Law School, accessed October 20, 2022, https://www.law.cornell.edu/wex/brady_rule#:~:text=A%20%22Brady%20material%22%20or%20evidence,the%20credibility%20of%20a%20witness.

analysis based on the time it took for the analysts to produce the report. Because WAPS is justified under the Public View doctrine, the collected information should be accessible to the public. When information is unavailable to the public, distrust and skepticism are likely to grow, particularly on the issue of WAPS. Cities already under Consent Decrees already have low levels of public trust.[539] At the same time, this also describes many of the cities with high violent crime rates. The low public trust is a known factor that has hindered law enforcement's capacity to solve violent crime.[540] If WAPS is not administered/controlled by police departments but by independent councils/committees or city council subcommittees, this could improve public support of WAPS. Elected representatives should decide the further details concerning the administration and distribution of WAPS data.

What are the constitutional limitations of a locally used WAPS system? Based on the constitutional analysis of existing precedents using the Court's interpretive approach, state and local governments should not be restricted from the persistent collection of activity in the public view for less than seven days. The camera resolution has been derived from commercially available products which fit under existing precedent. The mere collection of preexisting information reasonable people knowingly expose to the public cannot be considered a search. The imagery cannot reveal information inside structures. Without engaging in analysis, the imagery is no different from looking outside the window of flying aircraft. Once information shifts

[539] Matt Vasilogambros, "The Feds Are Investigating Local Police Departments Again. Here's What to Expect," Pew Charitable Trusts, May 3, 2021, accessed October 20, 2022 https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/05/03/the-feds-are-investigating-local-police-departments-again-heres-what-to-expect

[540] Daniel S. Lawrence, Nancy La Vigne, Jesse Jannetta, Jocelyn Fontaine, "Impact of the National Initiative for Building Community Trust and Justice on Police Administrative Outcomes," Urban Institute Justice Policy Center, August 2019, accessed October 20, 2022 https://www.urban.org/sites/default/files/publication/100707/impact_of_the_national_initiative_for_building_community_trust_and_justice_on_police_administrative_outcomes_2.pdf; Pamela M. Low, "Community Trust in Their Local Police Force," Silicon Valley Notebook: Vol. 16, Article 7, https://scholarcommons.scu.edu/svn/vol16/iss1/7; International Association of Chiefs of Police, "Building Trust Between the Police and the Citizens They Serve: An Internal Affairs Promising Practices Guide for Local Law Enforcement," Community Oriented Policing Services Department of Justice, October 16, 2009, accessed October 20, 2022, https://cops.usdoj.gov/RIC/Publications/cops-p170-pub.pdf

from unknown people over indiscriminate areas to persons or areas of interest following a report, probable cause must be established. The Court has not yet recognized the collective right to privacy. Therefore, the individual's right to be secure from unreasonable search or seizure remains the standing rule. If a collective right to privacy is recognized, the whole Fourth Amendment jurisprudence would be altered. Once probable cause has been established, the analysis may begin within the limits of the probable cause and subsequent warrants. The Constitution does not require recommendations concerning disclosure, data retention, and access, but they are highly encouraged to uphold the principles of representative democracy. The line between the Fourth Amendment and new technologies has been the protection of PII. PII has not been identified as the standard despite the legal practice of recognizing and seeking to protect it for over twenty years. They are articulating PII as the standard that provides clear guidelines for law enforcement practices and legal scholarship.

Further Research and Conclusion

It does not matter if the government's use of WAPS is or is not constitutional. The Constitution, in this case, interpretation of the Fourth Amendment, provides the floor for what the government cannot do. As many have seen with discussions and debates over social media access and claims of censorship or the lack thereof, the Constitution does not limit what private parties can do.[541] Because of this limited government understanding, private entities can and likely will use WAPS without the constitutional limitations being considered. There have been collisions between new technologies and how private parties and governments use said

[541] Jeffrey Rosen, Kate Klonick, David French, "What is Section 230?," National Constitution Center, We The People Podcast audio, June 4, 2020, https://constitutioncenter.org/news-debate/podcasts/what-is-section-230

technology. This includes software innovations like facial recognition,[542] predictive algorithms,[543] and encrypted data.[544] In the hardware[545] realm, where WAPS finds company, the extent to

[542] Bruce Schneier, "The Era Of Automatic Facial Recognition And Surveillance Is Here," Forbes, September 29, 2015, https://www.forbes.com/sites/bruceschneier/2015/09/29/the-era-of-automatic-facial-recognition-and-surveillance-is-here/?sh=630704044cfb accessed May 7, 2021/; Trevor Timm, "Think It's Cool Facebook Can Auto-Tag You in Pics? So Does the Government" The Guardian, June 27, 2015, https://www.theguardian.com/commentisfree/2015/jun/27/facebook-tag-pics-government accessed May 7, 2021.; Olivia Goldhill, "Facial Recognition Technology: Is Orwell's Fiction Our Reality?," The Telegraph, June 23, 2015, https://www.telegraph.co.uk/technology/11693965/Facial-recognition-technology-Is-Orwells-fiction-our-reality.html accessed May 7, 2021.; Alfred Ng, "Boston Votes to Ban Government Use of Facial Recognition," CNet.com, June 24, 2020, https://www.cnet.com/news/boston-votes-to-ban-government-use-of-facial-recognition/ accessed May 7, 2021.

[543] Laurie Clark, "How the Cambridge Analytica Scandal Unravelled," The New Statesman, October 15, 2020, https://www.newstatesman.com/science-tech/social-media/2020/10/how-cambridge-analytica-scandal-unravelled accessed May 7, 2021; Patty Neiberg, "Colorado Bill Prohibits Insurers from Using 'Discriminatory' Data, like Social Media and Credit Scores, to Set Rates," The Colorado Sun, May 4, 2021, https://coloradosun.com/2021/05/04/ccolorado-bill-discriminatory-insurance-rates/ accessed May 7, 2021.

[544] Chris Matyszczyk, "Privacy is Just for Crooks, says Enlightened Government Agency," ZDNet, May 7, 2021, https://www.zdnet.com/article/privacy-is-just-for-crooks-says-enlightened-government-agency/ accessed May 7, 2021.; Jack Nicas, "The Police Can Probably Break Into Your Phone," New York Times, October 21, 2020, https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html accessed May 7, 2021.; Riana Pfefferkorn, "The FBI is Mad Because It Keeps Getting Into Locked iPhones Without Apple's Help," TechCrunch, May 22, 2020, https://techcrunch.com/2020/05/22/the-fbi-is-mad-because-it-keeps-getting-into-locked-iphones-without-apples-help/ accessed May 7, 2021.

[545] "The Secret Surveillance Catalogue," The Intercept, https://theintercept.com/surveillance-catalogue/ accessed May 7, 2021.

which smartphones,[546] DNA tests,[547] video doorbells,[548] and drones,[549] just to name a few, can be used to collect data for legitimate government purposes is an active and growing realm. For example, if a private entity deploys higher resolution WAPS like ARGUS, they certainly could be equipped with facial recognition software and have the resolution to use it. Such a combination of technologies might disqualify otherwise acceptable government practices but not private entities with particular interests. One does not need to go too far into dystopian scenarios to imagine if such capabilities would be restrained.

In the movie Minority Report,[550] one possible example demonstrated where retinal scans were conducted persistently throughout public spaces. The private interest was personalized marketing. The public interests were the swift ability to locate specific individuals for criminal apprehension, or in the case of the film, precrime prevention. In 2021, the imagination of the 2002 film can seem eerily close to what was hypothetically imagined in 2054. An innocent

---

[546] Hamed Aleaziz and Caroline Haskins, "DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People," Buzzfeed News, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation accessed May 7, 2021; Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," New York Times, January 2s, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html accessed May 7, 2021.; Will Ockden, "How Your Phone Tracks Your Every Move" ABC Australia, August 16, 2015, https://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152?nw=0 accessed May 7, 2021.; Greg Moran, "Are Those Government Spy Planes Overhead?," San Diego Tribune, April 8, 2016, https://www.sandiegouniontribune.com/news/data-watch/sdut-spy-planes-2016apr08-htmlstory.html accessed May 7, 2021.

[547] Jonah Valdez, "After 41 years, DNA from Genealogy Database Leads to Arrest in Death of 79-Year-Old California Grandmother," The Mercury News, May 3, 2021, https://www.mercurynews.com/2021/05/03/new-mexico-man-arrested-in-1980-death-of-79-year-old-anaheim-woman/ accessed May 7, 2021.; David Lazarus, "Why Spend Billions for Ancestry's DNA Data If You Don't Plan to Use It?" Los Angeles Times, April 13, 2021, https://www.latimes.com/business/story/2021-04-13/column-blackstone-ancestry-genetic-privacy accessed May 7, 2021.; Virginia Hughes, "To Solve 3 Cold Cases, This Small County Got a DNA Crash Course," New York Times, May 3, 2021, https://www.nytimes.com/2021/05/03/science/cold-cases-genetic-genealogy.html accessed May 7, 2021. https://www.mercurynews.com/2021/05/03/new-mexico-man-arrested-in-1980-death-of-79-year-old-anaheim-woman/

[548] Declan McCullagh, "Doorbell Surveillance Networks Have Arrived. Should We Be Scared?," Reason Magazine, December 2019, https://reason.com/2019/11/21/doorbell-surveillance-networks-have-arrived-should-we-be-scared/ accessed May 7, 2021.

[549] Joseph J. Vacek. "The Next Frontier in Drone Law: Liability for Cybersecurity Negligence and Data Breaches for UAS Operators." *Campbell Law Review*. No. 1 (2017).

[550] MACH at the Movies, "From Face Scanning To Targeted Ads, Minority Report's Future Isn't Sci-Fi Anymore," NBC News, October 1, 2018, https://youtu.be/gcimRZF8g3Y accessed May 7, 2021.

search or mention of a specific pair of shoes on one's favorite online store and social media will likely start including advertisements for those shoes. A click on a bag of keto chips advertisement in social media feed and every other advertisement will show similar products. The concern over the ethical use of algorithms is the topic of numerous popular documentaries, ironically enough, on streaming sites that use those same kinds of algorithms to match subscribers' interest to more original programming. Among them, Jeff Orlowski's Social Dilemma paints what many would find a disturbing revelation of Big Data's capacity.

Who might be the private entities to field high-resolution WAPS? None other than large corporations like Alphabet Company, Google's parent company. Not because they are merely a popular conglomerate to malign but because their past behavior and present capacity make such a suggestion reasonable. Google's thirst for data is insatiable, and deploying WAPS over significant major cities would add more real-time detail for further marketing goals. From 2009 to April 2021, Google has maintained over 75% of the United States search engine market share.[551] We know as Google Earth was built by a company that the Central Intelligence Agency (CIA) and National Geospatial Agency (NGA) previously held partial ownership of and had almost exclusive contracts with military and intelligence entities.[552] Google's recent rollout of Timelapse on Google Earth demonstrates its continued commitment to developing imagery assets.[553] Due to populations continuing to concentrate in urban and suburban areas, fiscally sound models that could collect imagery on most of the United States population are not far-fetched. Present estimates suggest that 83% of the population lives in cities, a figure that is only growing over the forecasted decades.[554] Because populations are so concentrated, it is

[551] See Appendix A.
[552] Yasha Levine, "The CIA Helped Sell a Mapping Startup to Google. Now They Won't Tell Us Why," Pando.com, July 1, 2015, https://pando.com/2015/07/01/cia-foia-google-keyhole/ accessed May 7, 2021.
[553] Rebecca Moore, "Time flies in Google Earth's biggest update in years," Google Blog, April 15, 2021, https://blog.google/products/earth/timelapse-in-google-earth/ accessed May 7, 2021.
[554] Center for Sustainable Systems, "U.S. Cities Factsheet," University of Michigan, 2020, Pub. No. CSS09-06.

reasonable to believe that the world's largest data processing company would likely invest in technology that could collect location information on the population in a way difficult to limit by law. The purpose of this research is not to be concerned with the private or public operation of WAPS but rather to demonstrate that the issue of WAPS should not be avoided.

Suppose Alphabet, through a subsidiary, to not violate Antitrust laws, fielded fleets of WAPS over the majority population of the United States. They would maintain primary control over the collection assets and the data. However, with the knowledge that such assets were flying and collecting that proprietary information, government entities could and by all accounts via numerous subpoenas, collect the data to be used as law enforcement would deem necessary. This could be accomplished with the Third Party Doctrine or through mildly creative interpretations of the Stored Communications Act,[555] the law which was at issue in *Carpenter*.

The Third Party doctrine could be the gateway to much of the government's ability to co-opt the data collected from the new devices. It is worth pointing out that *Carpenter*'s refusal to extend Third Party doctrine to CSLI information was a win for civil libertarians. However, the lack of explanation beyond "unique nature" left the future Fourth Amendment interpretation to precedents from what many believe to be a bygone era, even if it was a few decades ago.

PSS has not limited its services to government clients only. At the 2008 Coca-Cola 600, PSS provided overwatch security. The event was not particularly active, and out of boredom, the PSS analysts and McNutt evaluated the sometimes hours-long struggle event attendees had in finding parking. By their estimate, if they were able to communicate with event organizers to find parking spaces for visitors and had each visitor purchased one extra soda, the event would have profited ten times more than the cost of the three-day event security.[556] Without further guidance from the Court on how to interpret the Fourth Amendment in the absence of legislation, the question of "what is privacy in the digital age?" will only grow.

[555] 18 U.S. Code § 2701-3
[556] Arthur Holland Michel, Kindle Edition, Location 1512.

This dissertation has asked and answered, “Is Wide-Area Persistent Surveillance by State and Local Governments Constitutional?” It has demonstrated why analyzing WAPS is an important contribution to Public Law and American Politics more broadly. It has provided a brief historical background of the development of WAPS. It has presented the relevant constitutional doctrines to demonstrate the complexity and reasonable uncertainty surrounding WAPS. It has presented the development of the Equilibrium Adjustment, and Mosaic Theory approaches to Fourth Amendment interpretation by the leading scholars. It has applied the analysis from both sides to *Leaders of a Beautiful Struggle v. Baltimore Police Department* at the federal district trial court, federal court of appeals, and an en banc panel of the federal court of appeals. It has presented policy recommendations for states and locales to consider if they elect to deploy WAPS.

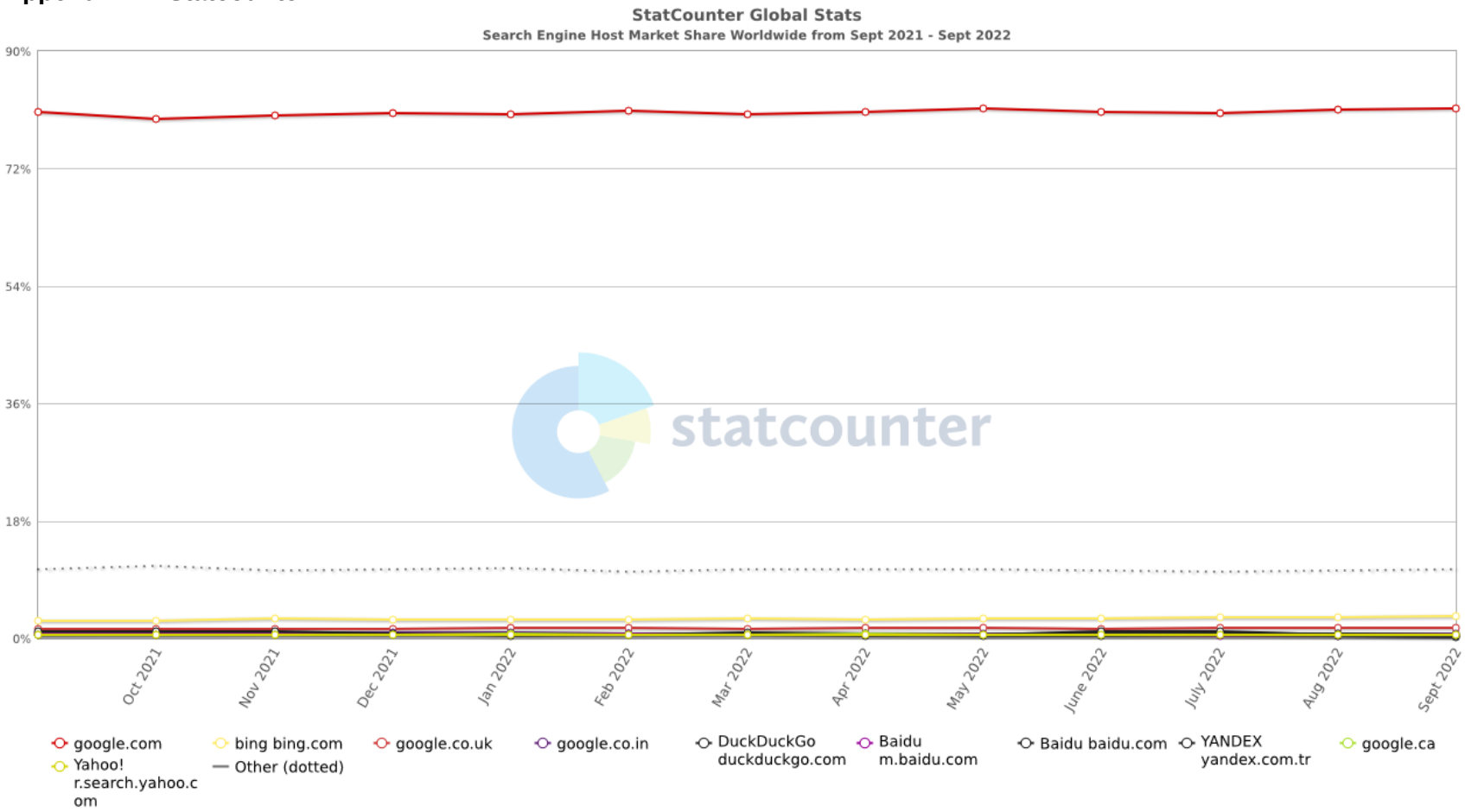
WAPS began as military technology inspired on a date night with a scientist. In less than a decade, it became one of the most valuable platforms in the United States military’s arsenal to combat the widespread use of improvised explosive devices in the Global War on Terror. Following the success of WAPS abroad, Ross McNutt brought it home with hopes of improving safety in communities and improving efficiency in various industries. After several short pilot programs across the United States and Mexico City, with the funding of criminal justice-oriented philanthropy, the AIR program was designed and deployed to the city of Baltimore. Due in part to the secretive nature of WAPS being used in 2016, civil rights groups were concerned about the capabilities of a potential all-seeing eye watching everyone all the time across Baltimore.

Once the issue of WAPS was before the Courts, WAPS demonstrated the conflicting approaches to Fourth Amendment interpretations resulting in completely opposing results. Based on Supreme Court precedents from the last century, no fewer than six different Fourth Amendment doctrines and two major competing theories applied to the constitutional question of WAPS. Well-meaning, earnest scholars and judges may land on opposing opinions of WAPS. However, based on the clear rulings of the Supreme Court and the sequential approach of

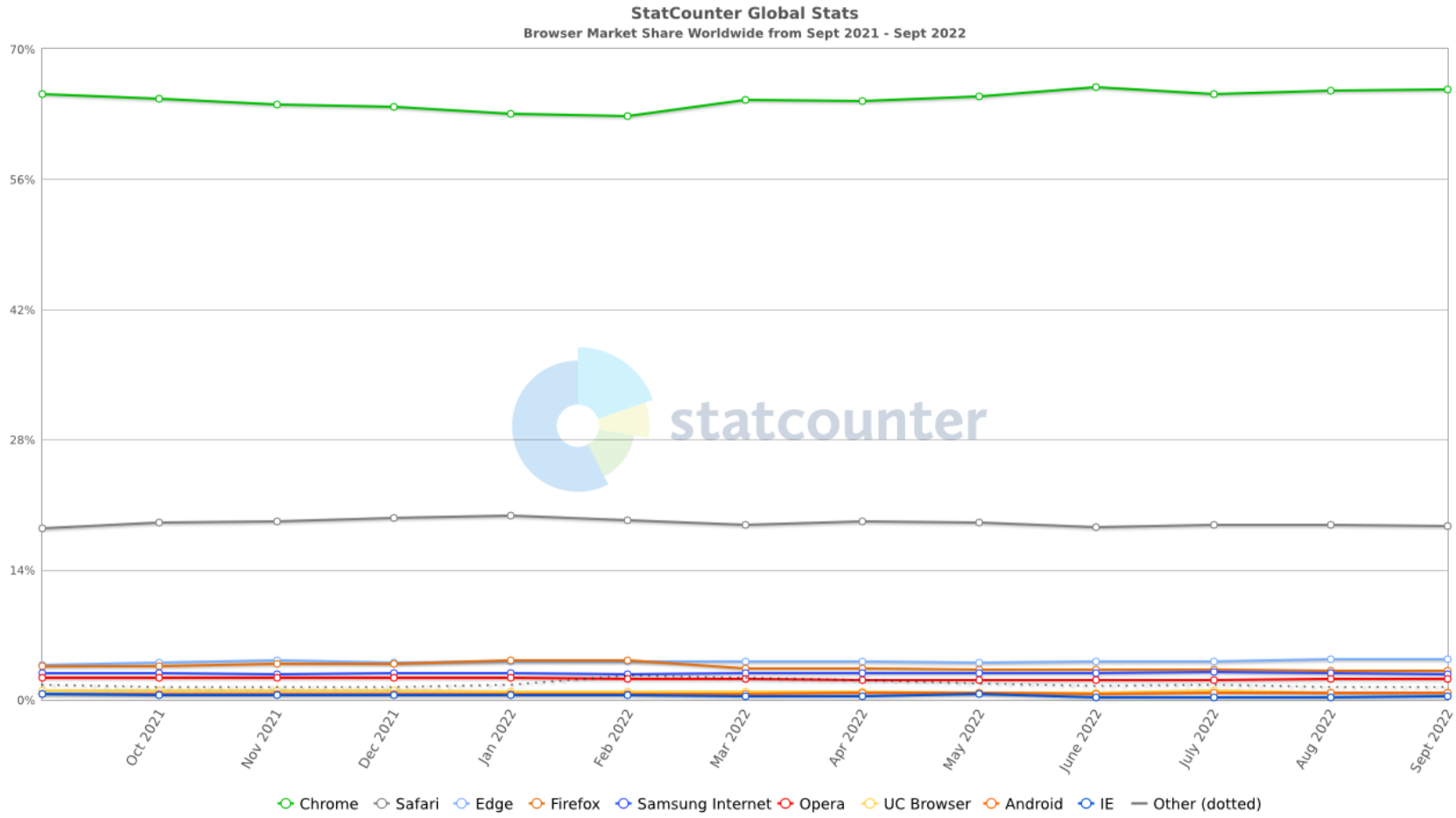
Fourth Amendment interpretation, WAPS can be constitutional. If the Courts adopt the Mosaic Theory, they will initiate a paradigm shift in the law enforcement investigation process, and the impermissibility of WAPS would be among the minor results. The judgment of the Courts relied upon whether the judges continued to use the sequential approach or if they adopted the Mosaic Theory.

Based on the clear decisions of the Supreme Court, WAPS can be constitutional without major difficulty in protecting the privacy rights of individuals, in as much as the existing precedents guide. So long as no analysis of WAPS data happens without probable cause, there are no unreasonable searches or seizures from aerial photography. This is regardless of the image's resolution, the duration of the collection, or the times of day the images are collected. At the most cautious level, there should not be more than six days of continuous data collection. As long as the analysis of WAPS is preceded by probable cause, no individual can be identified unreasonably. WAPS does not produce location information like CSLI data or a GPS tracking device, which actively produces new information for the duration of its operation. WAPS is limited to passive information in the public view. These differences do not mean there should not be limitations on WAPS. Prudence would encourage government operators and administrators of WAPS to provide public access to the public information collected. With that in mind, I recommend state and local governments seeking to deploy WAPS to operate and administer it outside of law enforcement control. In addition, such programs should be sufficiently funded and staffed to provide the public to make information requests of the WAPS data for a range of public interest causes in addition to public safety.

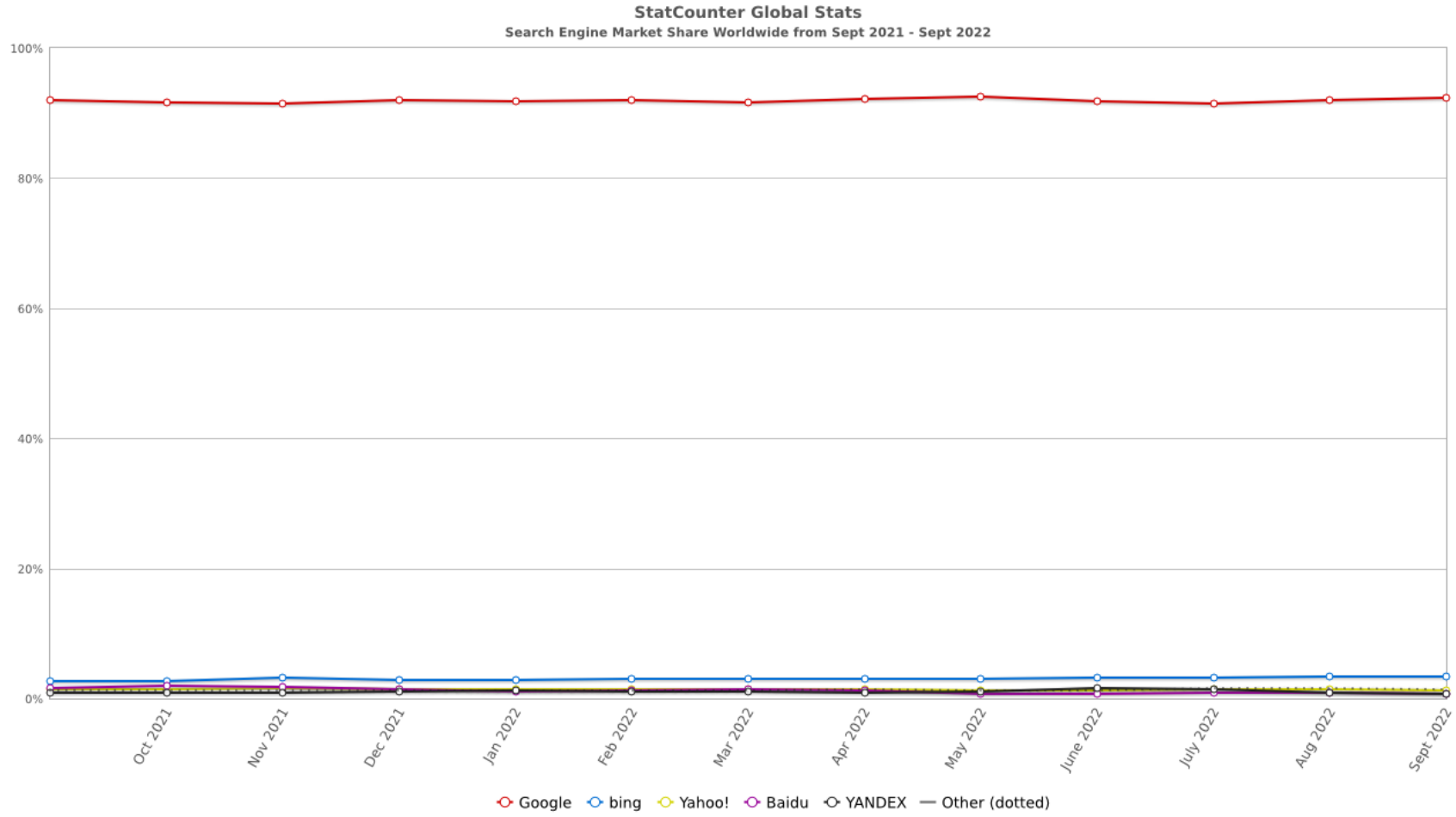
Appendix A - Statcounter



Search Engine/Country	Google google.com	Bing bing.com	Google google.co.uk	Google google.co.in	DuckDuckGo duckduckgo.com	Google google.ca
Market Share	81.16%	3.32%	1.57%	0.77%	0.63%	0.59%



Browser	Chrome (Google)	Safari (Apple)	Edge (Microsoft)	Firefox (Mozilla)	Samsung Internet (Samsung)	Opera
Market Share	65.7%	18.66%	4.32%	3.14%	2.75%	2.25%



Search Engine	Google	Bing	Yahoo!	YANDEX (Russia)	Baidu (China)	DuckDuckGo
Market Share	92.42%	3.45%	1.32%	0.79%	0.65%	0.63%

Bibliography

Adler v. Board of Education of City of New York. 1952. 342 U.S. 485 (United States Supreme Court, 3 March).

Aldhous, Peter. 2017. "Here's How BuzzFeed News Trained A Computer To Search For Hidden Spy Planes." *BuzzFeed News*, 7 August. Accessed July 25, 2021. https://www.buzzfeednews.com/article/peteraldhous/hidden-spy-planes.

Almeida-Sanchez v. United States. 1973. 413 U.S. 266 (US Supreme Court, 21 June).

Al-Shakarji, N M, Bunyak Seetharaman, and K Palanianppan. 2019. "Robust Multi-object Tracking for Wide Area Motion Imagery." IEEE, 9 May. Accessed June 20, 2020. https://ieeexplore.ieee.org/document/8707377.

Aly, Hesham. 2016. "How the Military Can Integrate Unmanned Aerial Systems in the Civil Reserve Air Fleet." Air University. Accessed May 19, 2019. https://apps.dtic.mil/sti/citations/AD1040989.

Amazon Web Services. 2021. "Amazon S3 Simple Storage Service Pricing - Amazon Web Services." *AWS.* Accessed July 21, 2021. https://aws.amazon.com/s3/pricing/.

American Civil Liberties Union. 2020. "Leaders of a Beautiful Struggle v. Baltimore Police Department." *ACLU.* 8 June. Accessed July 18, 2020. https://www.aclu.org/cases/leaders-beautiful-struggle-v-baltimore-police-department.

Andrew R. Morral, Terry L. Schell, Brandon Crosby, Rosanna Smart, Rose Kerber, Justin Lee. 2021. *Preliminary Findings from the Aerial Investigation Research Pilot Program.* Santa Monica: RAND Corporation.

Anthony, Sebastian. 2013. "DARPA shows off 1.8-gigapixel surveillance drone, can spot a terrorist from 20000 feet." *ExtremeTech.* 28 January. Accessed April 15, 2021.

https://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet.

Arizona v. Hicks. 1987. 480 U.S. 321 (United States Supreme Court, 3 March).

Asari, Vijayan K., ed. 2013. *Wide Area Surveillance: Real-time Motion Detection Systems.* Springer Berlin Heidelberg. Accessed June 20, 2020. https://link.springer.com/book/10.1007/978-3-642-37841-6.

Austen, Ian. 2000. "For the Spy in the Sky, New Eyes." *New York Times.* 20 June. Accessed April 24, 2021. https://www.cds.caltech.edu/~murray/courses/cds101/fa02/caltech/steadycam.html.

Barron v. Baltimore. 1833. 32 U.S. (7 Pet.) 243 (United States Supreme Court, 16 February).

Bates, Jonathan. 2022. "Current Unmanned Aircraft State Law Landscape." *National Conference of State Legislatures.* 26 October. Accessed January 18, 2023. https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

Berger v. New York. 1967. 388 U.S. 41 (United States Supreme Court, 12 June).

2020. *Eye in the Sky - Inside America's 24-Hours Airspace Surveillance System.* Directed by Doc Bites. Accessed July, 2021.

Blasch, E., G. Seetharaman, K. Palaniappan, H Ling, and E. Chen. n.d. "Wide-Area Motion Imagery (WAMI) Exploitation Tools for Enhanced Situation Awareness." IEEE. Accessed June 20, 2020. https://ieeexplore.ieee.org/document/6528198.

Board of Education of Independent School District No. 92 of Pottawatomie City v. Earls. 2002. 536 U.S. 822 (United States Supreme Court, 27 June).

Bond v. United States. 2000. 529 U.S. 334 (United States Supreme Court, 17 April).

Boyd v. United States. 1886. 116 U.S. 616 (United States Supreme Court, 1 February).

Breyer, Stephen. 2006. *Active Liberty: Interpreting Our Democratic Constitution.* New York: Knopf Doubleday Publishing Group. Accessed February 26, 2021.

Bridgens, Gary. 2021. "Demystifying Reliance Interests in Judicial Review of Regulatory Change." *George Mason Law Review* 29 (1): 411-446. Accessed September 21, 2022. https://lawreview.gmu.edu/print__issues/demystifying-reliance-interests-in-judicial-review-of-regulatory-change/.

Brigham City v. Stuart. 2006. 547 U.S. 398 (United States Supreme Court, 22 May).

Buolamwini, Joy. 2017. "Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers." Massachusetts Institute of Technology. Accessed June 18, 2020. https://www.media.mit.edu/publications/full-gender-shades-thesis-17/.

California Highway Patrol. 2021. "Report to the Legislature SB719 Police Pursuits." Sacramento, CA: State of California, November. Accessed February 10, 2023. https://www.chp.ca.gov/Documents/2021%20SB%20719%20-%20Police%20Pursuits.pdf.

California v. Carney. 1985. 471 U.S. 386 (United States Supreme Court, 19 March).

California v. Ciraolo. 1986. 84-1513 (United States Supreme Court, 19 May).

California v. Greenwood. 1988. 486 U.S. 35 (United States Supreme Court, 16 May).

Camara v. Municipal Court. 1967. 92 (United States Supreme Court, 5 June).

Caniglia v. Strom. 2021. 593 U.S. ___ (United States Supreme Court, 17 May).

Cardwell v. Lewis. 1974. 417 U.S. 583 (United States Supreme Court, 17 June).

Carlson, Andrea. 2018. "Electric Eye: Mass Aerial Surveillance and the Fourth Amendment." *Illinois Journal of Law, Technology & Policy* 2018 (1): 167-198.

Carpenter v. United States. 2018. 16-402 (United States Supreme Court, 22 June).

Carroll v. United States. 1925. 267 U.S. 132 (United States Supreme Court, 2 March).

Cayman Compass. 2010. "The new face of intelligence." 4 July. Accessed January 7, 2023. https://www.caymancompass.com/2010/07/04/the-new-face-of-intelligence/.

Central Intelligence Agency v. Sims. 1985. 86-1075 (United States Supreme Court, 16 April).

Chandler v. Miller. 1997. 520 U.S. 305 (United States Supreme Court, 15 April).

City of Indianapolis v. Edmond. 2000. 531 U.S. 44 (US Supreme Court, 28 November).

Colorado v. Bannister. 1980. 449 U.S. 1 (United States Supreme Court, 20 October).

2011. *Commander's Handbook for Persistent Surveillance version 1.0.* Suffolk: Joint Warfighting Center Joint Doctrine Support Division.

Coolidge v. New Hampshire. 1971. 403 U.S. 443 (United States Supreme Court, 21 June).

Cooper v. California. 1967. 386 U.S. 58 (United States Supreme Court, 20 February).

Cotten, Ann. 2020. "Baltimore Aerial Investigation Research Project Findings from the Early Launch Community Survey." University of Baltimore Schaefer Center for Public Policy, June. Accessed June 29, 2021. https://68i.ab1.myftpupload.com/wp-content/uploads/2020/12/AIRCommunitySurvey-Summary-AllHCHP-FINAL.pdf.

Coughlin, Tom. 2019. "Digital Storage Projections For 2020, Part 1." *Forbes.* 21 December. Accessed April 24, 2021. https://www.forbes.com/sites/tomcoughlin/2019/12/21/digital-storage-projections-for-2020-part-1/?sh=5e082f31581c.

Cypher, Trish, and Colin Grinnell. 2007. "Governments Working Together: A Citizen's Guide to Joint Powers Agreements." California State Legislature Senate Local Government Committee, August. Accessed October 20, 2022. https://sgf.senate.ca.gov/sites/sgf.senate.ca.gov/files/GWTFinalversion2.pdf.

Daniel S. Lawrence, Nancy La Vigne, Jesse Jannetta, Jocelyn Fontaine. 2019. *Impact of the National Initiative for Building Community Trust and Justice on Police Administrative Outcomes.* Washington: Urban Institute.

de Montjoye, Yves-Alexandre, César A Hidalgo, Michel Verleysen, and Vincent Blondel. 2013. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* 3: 1-5. Accessed August 4, 2020. https://pubmed.ncbi.nlm.nih.gov/23524645/.

Department of Homeland Security Science and Technology. 2022. *TechNote: Computer Aided Dispatch Systems.* Washington: Department of Homeland Security.

District of Columbia v. Heller. 2008. 554 U.S. 570 (United States Supreme Court, 18 March).

Dobbs v. Jackson Women's Health Organization. 2022. 597 U.S. ____ (No. 19-1392) (United States Supreme Court, 24 June).

Dow Chemical Company v. United States. 1986. 84-1259 (United States Supreme Court, 19 May).

Fekkes, Cristina. 2009. "Defining Conditions for the Use of Persistent Surveillance." Navy Postgraduate School. Accessed June 25, 2020. https://calhoun.nps.edu/handle/10945/4444.

Ferguson, Andrew G. 2022. "Persistent Surveillance." *Alabama Law Review* Forthcoming. Accessed April 30, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071189.

Florence v. Board of Chosen Freeholders. 2012. 566 U.S. 318 (U.S. Supreme Court, 2 April).

Florida v. Riley. 1988. 87-764 (United States Supreme Court, 22 February).

Frank v. Maryland. 1959. 278 (United States Supreme Court, 4 May).

Friedman, Barry, and Max Isaacs. 2020. "Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program." The Policing Project at NYU Law, November. Accessed June 29, 2021. https://www.policingproject.org/s/AIR-Program-Audit-Report-vFINAL-reduced.pdf.

Garfield, Leanna. 2015. "The CIA's EarthViewer was basically the original Google Earth." *Business Insider.* 30 December. Accessed November 23, 2021. https://www.businessinsider.com/the-cias-earthviewer-was-the-original-google-earth-2015-11.

Gitlow v. New York. 1925. 268 U.S. 652 (United States Supreme Court, 8 June).

Gonzales v. Carhart. 2007. 550 U.S. 124 (United States Supreme Court, 18 April).

Gouré, Daniel. 2012. "Wide Area Persistent Surveillance Revolutionizes Tactical ISR." Lexington Institute, 28 November. Accessed June 23, 2020.

https://www.lexingtoninstitute.org/wide-area-persistent-surveillance-revolutionizes-tactical-isr/.

Grady v. North Carolina. 2015. 14-593 (United States Supreme Court, 30 March).

Gray, David. 2021. "Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies." *Southern Methodist University Science and Technology Law Review* 3-63.

Gray, David, and Danielle Citron. 2016. "A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy." *North Carolina Journal of Law & Technology* 381-430. Accessed July 9, 2021. http://scholarship.law.unc.edu/ncjolt/vol14/iss2/3.

Gray, David. 2019. "Collective Rights and the Fourth Amendment After Carpenter." *Maryland Law Review* 79 (1): 66-87. Accessed July 30, 2021. https://digitalcommons.law.umaryland.edu/mlr/vol79/iss1/4.

Gray, David. 2018. "Collective Standing under the Fourth Amendment." *Georgetown Law (American Criminal Law Review)* 55 (1): 77-104. Accessed April 30, 2022. https://www.law.georgetown.edu/american-criminal-law-review/in-print/volume-55-issue-1-winter-2018/collective-standing-under-the-fourth-amendment/.

—. 2017. *The Fourth Amendment in an Age of Surveillance.* Cambridge: Cambridge University Press. Accessed February 26, 2021. https://digitalcommons.law.umaryland.edu/books/111.

Gray, David, and Danielle Citron. 2013. "The Right to Quantitative Privacy." *Minnesota Law Review* 98: 62-144. Accessed May 14, 2021. https://ssrn.com/abstract=2228919.

Griswold v. Conneticut. 1965. 496 (United States Supreme Court, 7 June).

Harris v. Unites States. 1968. 390 U.S. 234 (United States Supreme Court, 5 March).

Harrison, Michael. 2020. *Professional Service Agreement Acceptance.* Memorandum of Understanding, Baltimore: Baltimore Police Department.

Hesham, Aly. 2016. *How the Military Can Integrate Unmanned Aerial Systems in the Civil Reserve Air Fleet.* Master's Thesis, Montgomery: Air University.

Hester v. United States. 1924. 243 (United States Supreme Court, 5 May).

Hogan, Todd. 2007. "The Persistent Intelligence, Surveillance, and Reconnaissance Dilemma: Can the Department of Defense Achieve Information Superiority?" U.S. Army Command and General Staff College. Accessed June 25, 2020. https://www.hsdl.org/?view&did=232599.

Holland Michel, Arthur. 2019. *Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All.* HarperCollins. Accessed June 9, 2020.

Hook, Gregory. 2022. "Baltimore Police Department Performance Audit Surveillance Equipment." Baltimore, Maryland: Maryland General Assembly Office of Legislative Audits, 17 June. Accessed October 13, 2022. https://dls.maryland.gov/pubs/prod/NoPblTabPDF/BPD-Surveillance22.pdf.

Horton v. California. 1990. 496 U.S. 128 (United States Supreme Court, 4 June).

Ian, Austen. 2000. "For the Spy in the Sky, New Eyes." *New York times*, 20 June. Accessed April 24, 2021. https://www.cds.caltech.edu/~murray/courses/cds101/fa02/caltech/steadycam.html.

Illinois v. Caballes. 2005. 543 U.S. 405 (United States Supreme Court, 24 January).

In re United States. 1989. 87-5383 (United States Court of Appeals, District of Columbia, 14 April).

2019. "Insights and Best Practices Intelligence Operations." Deployable Training Division of the Joint Chiefs of Staff. Accessed July 27, 2021. https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/intell_ops_fp.pdf.

International Association of Chiefs of Police. 2009. *Building Trust Between the Police and the Citizens They Serve: An Internal Affairs Promising Practices Guide for Local Law*

Enforcement. Government Report, Washington: Community Oriented Policing Services Department of Justice.

Jr., Martin Luther King. 1963. "Letter from Birmingham Jail." *Letter from Birmingham Jail.* August.

Kate Klonick, David French, interview by Jeffery Rosen. 2020. *What is Section 230?* (4 June).

Katz v. United States. 1967. 35 (United States Supreme Court, 18 December).

Kentucky v. King. 2011. 563 U.S. 452 (United States Supreme Court, 16 May).

Kerr, Orin. 2004. "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it." *George Washington Law Review* 72 (8). Accessed July 21, 2020. https://ssrn.com/abstract=421860.

Kerr, Orin. 2011. "An Equilibrium Adjustment Theory of the Fourth Amendment." *Harvard Law Review* 125 (476): 476-543. Accessed July 21, 2021. https://ssrn.com/abstract=1748222.

Kerr, Orin. 2016. "Do We Need a New Fourth Amendment?" *Michigan Law Review* 107 (951): 951-966. Accessed July 21, 2020. https://repository.law.umich.edu/mlr/vol107/iss6/5/.

Kerr, Orin. 2007. "Four Models of Fourth Amendment Protection." *Stanford Law Review* 60 (2): 503-552. Accessed May 20, 2021. http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2010/04/Kerr.pdf.

Kerr, Orin. 2018 Forthcoming. "Implementing Carpenter." In *The Digital Fourth Amendment*, Chapter 6. Oxford University Press. Accessed May 15, 2021. https://ssrn.com/abstract=3301257.

Kerr, Orin. 2011. "Katz Has Only One Step: The Irrelevance of Subjective Expectations." *Harvard Law Review* 125 (476): 113-134. Accessed July 21, 2021. https://lawreview.uchicago.edu/publication/katz-has-only-one-step-irrelevance-subjective-expectations-0#.

Kerr, Orin. 2009. "Do We Need a New Fourth Amendment?" *Michigan Law Review* 951-966.

Kerr, Orin. 2016. "The Effect of Legislation on Fourth Amendment Protection." *Michigan Law Review* 115 (1117): 1117-1165. Accessed July 21, 2020. https://ssrn.com/abstract=2819878.

Kerr, Orin. 2004. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution." *Michigan Law Review* 102 (5): 801-888. Accessed July 21, 2021. https://repository.law.umich.edu/mlr/vol102/iss5/1.

Kerr, Orin. 2012. "The Mosaic Theory of the Fourth Amendment." *Michigan Law Review* 111 (311): 311-354. Accessed July 21, 2020. https://ssrn.com/abstract=2032821.

Kerr, Orin. 2021. "The Questionable Objectivity of the Fourth Amendment Law." *Texas Law Review* 99 (447): 447-489. Accessed July 13, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3651475.

Kerr, Orin. 2014. "Why Courts Should Not Quantify Probable Cause." In *The Political Heart of Criminal Procedure: Essays on Themes of William J. Stuntz*. Cambridge University Press. Accessed July 21, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1797824.

Kimmons, Jeff, and Graham Gilmer. 2019. "Maintaining Advantage: Remaking PED for Today's Intelligence Needs." Maclean, Virginia: Booz Allen Hamilton. Accessed July 21, 2021. https://www.defenseone.com/media/ped-thought-piece-presentedby-booz-allen.pdf.

Kyllo v. United States. 2001. 99-8508 (United States Supreme Court, 11 June).

Lange v. California. 2021. 594 U.S. ___ (United States Supreme Court, 23 June).

Leaders of a Beautiful Struggle v. Baltimore Police Department. 2020. 20-1495 (United States Court of Appeals for the Fourth District, 5 November).

Leaders of a Beautiful Struggle v. Baltimore Police Department. 2021. 20-1495 (United States Court of Appeals for the Fourth Circuit, 24 June).

Lochner v. New York. 1905. 292 (United States Supreme Court, 17 April).

Madison, James. 2000. *Property.* Vol. 1, in *The Founders' Constitution*. University of Chicago Press. Accessed August 2, 2021. https://press-pubs.uchicago.edu/founders/documents/v1ch16s23.html.

Madison, James. 1962. "Property." In *The Papers of James Madison*, by William Hutchinson. Chicago: University of Chicago.

Mapp v. Ohio. 1961. 236 (United States Supreme Court, 19 June).

Maryland v King. 2013. 569 U.S. 435 (United States Supreme Court, 3 June).

McCulloch v. Maryland. 1819. (United States Supreme Court, 6 March).

McNeal, Gregory. 2014. "Drones and Aerial Surveillance: Considerations for Legislators." Brookings Institution, November. Accessed April 2, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523041.

McNeal, Gregory. 2015. "Government-Operated Drones and Data Retention." *Washington & Lee Law Review* 72 (3): 1139-1159. Accessed April 2, 2019.

McNutt, Ross. 2014. "Wide Area Surveillance in Support of Law Enforcement." Xenia, Ohio: Persistent Surveillance Systems, January. Accessed June 25, 2020. https://info.publicintelligence.net/PSS-WideAreaSurveillance.pdf.

Menthe, Lance, Dahlia A Goldfeld, Abbie Tingstad, Sherrill Lingel, Edward Geist, Donald Brunk, Amanda Wicker, et al. 2021. "Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 2, Technical Analysis and Supporting Material." Santa Monica, California: RAND Corporation. Accessed February 1, 2023. https://www.rand.org/pubs/research_reports/RRA341-2.html.

Meyer v. Nebraska. 1923. 262 U.S. 678 (United States Supreme Court, 4 June).

Michel, Arthur Holland. 2019. *Eyes in the Sky: The Secret Rise of Gorgon Stare and How it Will Watch Us All.* Boston: Mariner Books.

Michigan Department of State Police. 1990. 88-1897 (United States Supreme Court, 14 June).

Minnesota v. Olson. 1990. 495 U.S. 91 (United States Supreme Court, 18 April).

Mitchell v. Wisconsin. 2019. 588 U.S. ___ (United States Supreme Court, 27 June).

Morral, Andrew, Terry Schell, Brandon Crosby, Rosanna Smart, Rose Kerber, and Justin Lee. 2021. "Preliminary Findings from the Aerial Investigation Research Pilot Program." Santa Monica, California: Rand Corporation. Accessed May 9, 2021. https://www.rand.org/pubs/research_reports/RRA1131-1.html.

Nagy, Brandon. 2014. "Why They Can Watch You: Assessing the Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement." *Berkeley Technology Law Journal* 29: 135-174. Accessed April 15, 2021. https://ssrn.com/abstract=2429092.

National Association for the Advancement of Colored People v. Alabama. 1958. 357 U.S. 449 (United States Supreme Court, 30 June).

National Association for the Advancment of Colored People v. Button. 1963. 371 U.S. 415 (United States Supreme Court, 14 January).

National Treasure Employees Union v. Von Raab. 1989. 489 U.S. 656 (United States Supreme Court, 21 March).

New Jersey v. T.L.O. 1985. 469 U.S. 351 (US Supreme Court, 15 January).

New York v. Belton. 1981. 453 U.S. 454 (United States Supreme Court, 1 July).

New York v. Class. 1986. 475 U.S. 106 (United States Supreme Court, 25 February).

Oliver v. United States. 1986. 466 U.S. 170 (United States Supreme Court, 17 April).

Olmestead v. United States. 1928. 493 (United States Supreme Court, 4 June).

Opilo, Emily. 2020. "Spy Plane Not Likely to Fly over Baltimore Again, Mayor Says." *Baltimore Sun*, 28 December. Accessed July 7, 2021. https://www.baltimoresun.com/politics/bs-md-pol-brandon-scott-interview-20201228-ti75hqctsffgrbyggpzdz2xtgm-story.html.

Pavletic, John. 2018. "The Fourth Amendment in the Age of Persistent Aerial Surveillance." *Criminal Law & Criminology* 108 (1). https://scholarlycommons.law.northwestern.edu/jclc/vol108/iss1/4.

Philip, R C, S Ram, X Gao, and J J Rodriguez. 2014. "A Comparison of Tracking Algorithm Performance for Objects in Wide Area Imagery." IEEE, 1 May. Accessed June 20, 2020. https://ieeexplore.ieee.org/document/6806041.

Police Commissioner Michael S. Harrison. 2020. "Police Commissioner Michael S. Harrison to the Honorable President nad Members of hte Board of Estimates." *Professional Service Agreement Acceptance (Memorandum of Understanding).* Baltimore: Baltimore Police Department, 17 March.

Pritt, M D, and K J LaTourette. 2012. "Georegistration of Multiple-Camera Wide Area Motion Imagery." IEEE International Geoscience and Remote Sensing Symposium. Accessed June 20, 2020. https://ieeexplore.ieee.org/document/6351174.

Prokaj, J, and G Medioni. 2014. "Persistent Tracking for Wide Area Aerial Surveillance." IEEE, 25 September. Accessed June 20, 2020. https://ieeexplore.ieee.org/abstract/document/6909551.

Rainey, James. 2014. "Sheriff's secret air surveillance of Compton sparks outrage." *Los Angeles Times*, 23 April. Accessed July 19, 2022. https://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html.

Rakas v. Illinois. 1978. 77-5781 (United States Supreme Court, 5 December).

Ratches, James A, Richard Chait, and John W Lyons. 2013. *DTP-100: Some Recent Sensor-Related Army Critical Technology Events.* National Defense University Press. Accessed June 23, 2020. https://ndupress.ndu.edu/Portals/68/Documents/DefenseTechnologyPapers/DTP-100.pdf?ver=2017-06-22-143033-827.

Rateches, James A, Richard Chait, and John W Lyons. 2013. *DTP-100: Some Recent Sensor-Related Army.* White Paper, Washington D.C.: National Defense University Press.

Rector, Kevin. 2016. "Cummings: Commissioner Davis 'apologized profusely' for not disclosing surveillance program." *Baltimore Sun*, 16 September: https://www.baltimoresun.com/news/crime/bs-md-ci-cummings-davis-meeting-20160902-story.html.

Reel, Monte. 2016. "Secret Cameras Record Baltimore's Every Move From Above." *Bloomberg.com*, 23 August. Accessed January 7, 2023. https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.

Richards, Neil. 2013. "The Dangers of Surveillance." *Harvard Law Review* 126 (1934): 1934-1965. Accessed May 3, 2022. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf.

Richards, Neil. 2006. "The Information Privacy Law Project." *Georgetown Law Journal* 1087-1140.

Riley v. California. 2014. 13-132 (United States Supreme Court, 25 June).

Roberts v. U.S. Jaycees. 1984. 468 U.S. 609 (US Supreme Court, 3 July).

Robertson, Adi. 2012. "Homeland Security Using Military Wide-Area Camera to Scan Miles of the Us Border at Once." *The Verge*, 2 April. Accessed July 27, 2021. https://www.theverge.com/2012/4/2/2919677/homeland-security-kestrel-surveillance-camera-us-mexico-border.

Rosanna Smart, Andrew R. Morral, Terry L. Schell. 2022. *Evaluating Baltimore's Aerial Investigation Research Pilot Program.* Santa Monica: RAND Corportation.

Samson v. California. 2006. 547 U.S. 855 (United States Supreme Court, 19 June).

Santhaseelan, V., and V. K. Asari. 2013. "Tracking in Wide Area Motion Imagery Using Phase Vector Fields." IEEE. Accessed June 20, 2020. https://ieeexplore.ieee.org/document/6595967.

Schmitt, Daniel. 2006. "Automated Knowledge Generation with Persistent Video Surveillance." Air University. Accessed June 25, 2020. https://scholar.afit.edu/cgi/viewcontent.cgi?article=3560&context=etd.

Silverman v. United States. 1961. 365 U.S. 505 (United States Supreme Court, 6 March).

Skinner v. Railway Labor Executives Association. 1989. 489 U.S. 602 (United States Supreme Court, 21 March).

Slobogin, Christopher. 2012. "An Original Take on Originalism." *Harvard Law Review* 125 (476): 14-22. Accessed April 19, 2022. https://harvardlawreview.org/2012/01/an-original-take-on-originalism/.

Slobogin, Christopher. 2010. "Government Dragnets." *Law and Contemporary Problems* 73 (107): 107-143. Accessed November 8, 2021. https://scholarship.law.vanderbilt.edu/faculty-publications/250.

Slobogin, Christopher. 2012. "Is the Fourth Amendment Relevant in a Technological Age?" In *The Future of The Constitution*. Washington, D.C.: Brookings Institute. Accessed November 8, 2021. https://www.brookings.edu/research/is-the-fourth-amendment-relevant-in-a-technological-age/.

Slobogin, Christopher. 2012. "Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory." *Duke Journal of Constitutional Law & Public Policy* 8 (1): 1-37. Accessed June 29, 2021. https://scholarship.law.duke.edu/djclpp/vol8/iss1/1.

Slobogin, Christopher. 2016. "Policing as Administration." *University of Pennsylvania Law Review* 165 (91): 91-152. Accessed May 18, 2022. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss1/3.

Slobogin, Christopher. 2017. "Policing, Databases, and Surveillance." *Criminology, Criminal Justice, Law & Society* 70-84.

Slobogin, Christopher. 2003. "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity." *Mississippi Law Journal* 72: 213-315. Accessed July 21, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=364600.

Slobogin, Christopher. 2021. "Suspectless Searches." *Vanderbuilt Law Research Paper Series* 1-17.

Smart, Rosanna, Andrew Morral, and Terry Schell. 2022. "Evaluating Baltimore's Aerial Investigation Research Pilot Program." Santa Monica, California: RAND Corporation. Accessed June 6, 2022. https://www.rand.org/pubs/research_reports/RRA1131-2.html.

Smith v. Maryland. 1979. 78-5374 (United States Supreme Court, 20 June).

Sotomayor, Sonia, interview by Scott Pelley. 2013. *Constitution: A living document or not?* CBS News, (13 January). https://youtu.be/kHvgiEWH6A4.

Spraul, Hartung, and T Schuchert. 2018. "Persistent Multiple Hypothesis Tracking for Wide Area Motion Imagery." IEEE, 22 February. Accessed June 20, 2020. https://ieeexplore.ieee.org/abstract/document/8296460.

State v. Blue. 2016. 246 N.C. App. 259 (Court of Appeals of North Carolina, 15 March).

Texas v. Brown. 1983. 460 U.S. 730 (United States Supreme Court, 19 April).

Thakkar, Rahul. 2012. "A Primer for Dissemination Services for Wide Area Motion Imagery." Open Geospatial Consortium, 5 December. Accessed June 20, 2020. https://portal.ogc.org/files/?artifact_id=50485.

Trish Cypher, Colin Grinnell. 2007. *Governments Working Together: A Citizen's Guide to Joint Powers Agreements.* Sacramento: California State Legislature Senate Local Government Committee.

U.S. Joint Forces Command. 2011. "Commander's Handbook for Persistent Surveillance." Joint Warfighting Center. Accessed April 23, 2021. https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/surveillance_hbk.pdf.

United States Air Force. 2015. "Air Force Distributed Common Ground System Fact Sheet." 13 October. Accessed July 21, 2021. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/.

—. 2015. "MQ-1B Predator > Air Force > Fact Sheet Display." *AF.mil.* September. Accessed July 21, 2021. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/.

—. 2012. "MQ-9 Reaper > Air Force > Fact Sheet Display." *AF.mil.* March. Accessed July 27, 2021. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/.

United States Joint Forces Command. 2011. "Commander's Handbook for Persistent Surveillance version 1.0." Joint Warfighting Center Joint Doctrine Support Division, June. Accessed April 23, 2021. https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/surveillance_hbk.pdf.

United States v. Brignoni-Ponce. 1975. 422 U.S. 878 (United States Supreme Court, 30 June).

United States v. Bucci. 2009. 07-2376 (United States Court of Appeals,First Circuit, 11 September).

United States v. Causby. 1946. 328 U.S. 256 (United States Supreme Court, 27 May).

United States v. Chatrie. 2022. 3:19-cr-130 (District Court, E.D. Virginia, 19 August).

United States v. Cuevas-Sanchez. 1987. 86-1665 (United States Court of Appeals, Fifth Circuit, 29 June).

United States v. Dunn. 1987. 480 U.S. 294 (United States Supreme Court, 3 March).

United States v. Flores-Montano. 2004. 541 U.S. 149 (US Supreme Court, 30 March).

United States v. Graham. 2016. 12-4659 (United States Court of Appeals for the Fourth Circuit, 31 May).

United States v. Houston. 2016. 14-5800 (United States Court of Appeals, Sixth Circuit, 8 February).

United States v. Jackson. 2000. 99-6090 (United States Court of Appeals, Tenth Circuit, 2 June).

United States v. Jacobsen. 1984. 466 U.S. 109 (United States Supreme Court, 2 April).

United States v. Jones. 2012. 10-1259 (United States Supreme Court, 23 January).

United States v. Karo. 1984. 83-850 (United States Supreme Court, 3 July).

United States v. Knights. 2001. 534 U.S. 112 (United States Supreme Court, 10 December).

United States v. Knotts. 1983. 81-1802 (United States Supreme Court, 2 March).

United States v. Martinez-Fuerte. 1976. 74-1560 (United States Supreme Court, 6 July).

United States v. Maynard. 2010. 08-3030 (US Court of Appeals for the District of Columbia, 6 August).

United States v. Miller. 1976. 74-1179 (United States Supreme Court, 21 April).

United States v. Nerber. 2000. 99-30161 (United States Court of Appeals,Ninth Circuit, 24 August).

United States v. Tuggle. 2021. 20-2352 (United States Court of Appeals for the Seventh Circuit, 14 July).

United States v. Vankesteren. 2009. 08-4110 (United States Court of Appeals, Fourth Circuit, 8 January).

Urban Institute. 2022. *Project State and Local Backgrounders: Criminal Justice Expenditures: Police, Corrections, and Courts.* Washington: Urban Institute.

Vacek, Joseph J. 2017. "The Next Frontier in Drone Law: Liability for Cybersecurity Negligence and Data Breaches for UAS Operators." *Campbell Law Review* 135-164.

Vemonia School District 47J v. Acton. 1995. 515 U.S. 646 (United States Supreme Court, 21 June).

Walsh, David. 2018. "EMARSS: The Hawker Beechcraft Turned Spy Plane." *Aviation Today*, 30 May. Accessed July 27, 2021. http://interactive.aviationtoday.com/emarss-the-hawker-beechcraft-turned-spy-plane/.

Warren, Samuel, and Louis Brandeis. 1890. "The Right of Privacy." *Harvard Law Review* 4 (5): 193-220. Accessed October 31, 2016. http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C.

White House. 2015. "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems." Washington, D.C.: White House, 15 February. Accessed July 28, 2021. https://www.govinfo.gov/content/pkg/DCPD-201500103/pdf/DCPD-201500103.pdf.

Williamson v. Lee Optical. 1955. 348 U.S. 483 (United States Supreme Court, 28 March).

Wolf v. Colorado. 1949. 17 (United States Supreme Court, 27 June).

Worthman, Paul. 1969. *Satellite Camera Manuals.* Memorandum, Washington D.C.: National Reconnaissance Office.

Zuboff, Shoshana. 2020. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs.