EYES IN THE SKY: THE DANGERS OF DRAGNET GOVERNMENT SURVEILLANCE, THE INADEQUACY OF THE MOSAIC THEORY, AND THE NEED FOR A LEGISLATIVE SOLUTION

*Robert Donald Fairbanks**

ABSTRACT

Modern, dragnet government surveillance is becoming increasingly common in the United States. The development of modern technology has enabled such surveillance, allowing the government to learn and store more about us than ever before. The growing prevalence of this form of surveillance comes at a significant cost to all. But unsurprisingly, the greatest cost is borne by the groups most marginalized in our society already. It is thus imperative, both to maintain a functioning society and create a more just one, to address this issue. Courts have recently started to use the Fourth Amendment as a regulatory force on this dangerous surveillance. However, the Fourth Amendment and its jurisprudence were not meant to cover government action

* This Note was originally drafted for Professor Paul Schwartz's Topics in Privacy and Security Law class in Fall 2021 at the University of California, Berkeley, School of Law. Since it was selected and edited for publication, there have been significant additions to the literature on this topic—a non-exhaustive list includes Elizabeth N. Jones's Crim Pro Rewired: Why Current Police Practices Require Candor in the Classroom; Matthew Tokson's Telephone Pole Cameras Under Fourth Amendment Law and The Carpenter Test as a Transformation of Fourth Amendment Law; Andrew Guthrie Ferguson's Persistent Surveillance, Why Digital Policing is Different, and Digital Rummaging, and Barry Friedman's Lawless Surveillance. I am grateful to the editors of the Albany Law Journal of Science & Technology for all their hard work to publish this Note. I also owe a great deal of thanks to Professor Schwartz, not only for his help with my paper and for introducing our class to the preeminent scholars in the field (a group of which he is undoubtedly a member), but also for his humour, kindness, and empathy during the pandemic. Lastly, I would be remiss if I failed to credit Mckenzie Robinson, who has read this Note more times than anybody ever has and likely ever will, for all her contributions.

of this kind. Thus, the primary solution of courts, the mosaic theory, does not address the problem well. This is demonstrated in *Leaders of a Beautiful Struggle*, a recent Fourth Circuit case where the court ruled on the constitutionality of Baltimore's aerial surveillance program. Problematically, judicial action in this area could lead to legislative inaction. And it is the legislature that is best positioned to address the issue. The legislature is better able to craft policies that balance the competing needs of government surveillance and civil liberty and enact legal regimes that reflect respect for everyone's privacy. And the legislature must do this soon.

INTRODUCTION

In the center of town, a grand tower was erected
From where the Eyemonger could watch so all were protected
From high up above, he could see everywhere.
He could see down each street and into every town square.[1]

Modern technology has made the world unrecognizable from what it was for most of human history. Government surveillance has become so pervasive that it has even found itself the subject of a children's book.[2] While concerns about government surveillance are nothing new,[3] the fears that have been written about for so long are now becoming a reality. Using a wide array of techniques and technologies, the government can track, listen to, and watch almost anyone it wants.[4] And government surveillance is increasingly taking the form of dragnet surveillance, where huge groups of people—entire cities—are swept into the surveillance apparatus indiscriminately.[5] Until recently, the powers that be have done seemingly little to prevent this development.[6] But courts have recently started to act, using

---

[1] Daniel Solove, EYEMONGER (2020).

[2] *See id.*

[3] *See, e.g.,* GEORGE ORWELL, 1984 (Signet Classics 1977) (emphasizing a historical concern surrounding government surveillance).

[4] Mark Mazzetti et. al., *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Dec. 8, 2022), https://nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[5] Ed Pilkington, *US immigration agency operates vast surveillance dragnet, study finds*, THE GUARDIAN (May 10, 2022, 7:00 AM), https://theguardian.com/world/2022/may/10/us-immigration-agency-ice-domestic-surveillance-study.

[6] *See* Exec. Order No. 14086, 28 C.F.R. § 201 (2022).

the Fourth Amendment to limit some of these practices.[7]

However, many of the dragnet surveillance techniques do not easily fit the Fourth Amendment. The world looks very different today than it did in 1792. While courts have ably adapted the Fourth Amendment to many modern developments, it is possible that the dragnet surveillance techniques modern technology enables are so far removed from the surveillance imaginable at the time the Fourth Amendment was written, they cannot fit the Fourth Amendment framework. This Note argues that courts' recent efforts in this area have been misguided. It is a mistake to contort traditional Fourth Amendment analyses to fit modern dragnet surveillance techniques; the predominant responsibility for addressing the serious issues modern surveillance techniques pose must lie with the legislature.

Part I discusses the significant and growing prevalence of government surveillance and how the mosaic theory developed as an attempt by the courts to address subsequent privacy concerns. Part II uses *Leaders of a Beautiful Struggle v. Baltimore Police Department* as a case study of how courts apply the mosaic theory to dragnet government surveillance. Then, Part II considers the problems that arise from the Fourth Circuit's application of the mosaic theory and concludes that the mosaic theory is a poor answer to a serious problem. Part III provides an alternative to the mosaic theory and argues that a legislative solution would be a better answer to the threats posed by modern dragnet surveillance techniques.

PART I:

In 1983, the Police told us exactly what the less musically focused police were going to do. They warned that "every breath you take, and every move you make, every bond you break, every step you take, [they'll] be watching you."[8] Their *1984*-esque fears[9] were not totally realized in 1983, but those fears have certainly come to pass in 2022.

Due to technological advances, dragnet government surveillance is more prevalent than ever before.[10] Video

---

[7] *See* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 3 (2020).

[8] THE POLICE, EVERY BREATH YOU TAKE (A&M 1983).

[9] *See generally* ORWELL, *supra* note 3 (exploring the dangers of broad, unchecked government oversight).

[10] *See* Danielle Citron & David Gray, *A Shattered Looking Glass: The Pitfalls*

surveillance in public spaces has been integrated into "a larger system of databases and algorithmic processing with the aim of achieving forms of anticipatory, preemptive policing."[11] Governments have "invested heavily in . . . biometrics; flying drone cameras, including micro air vehicles; and other robotics; and there has been a general extension of military and quasi-military technology into urban space as part of global surveillance surges."[12] The government can track you, hear you, and see you almost anywhere, but especially in public places.[13] In the words of Christopher Slobogin, "What was once unthinkable or at least highly uneconomical is now possible with the flick of a mouse or the push of a button."[14] But why does that matter? Government surveillance is just meant to catch wrongdoers, so you don't have anything to worry about, right? Not quite.

As Neil Richards explains, "[P]rivacy isn't about hiding dark secrets."[15] This is for three main reasons: (1) everyone has secrets they rightfully wish to preserve, (2) human information provides power, and (3) privacy "matters not just to individuals but to the broader fabric of our society as a whole."[16] Priscilla Regan makes a similar argument for the importance of privacy, not just for individuals, but for society as a whole because privacy serves "common, public, and collective purposes."[17] Scott Skinner-Thompson points out that the lack of privacy due to surveillance chills freedom of speech and association.[18] And at a more

---

and Potential of the Mosaic Theory of Fourth Amendment Privacy, 14 N.C. J. L. & TECH. 381, 385–87 (2013).

[11] TORIN MONAHAN & DAVID MURAKAMI WOOD, SURVEILLANCE STUDIES: A READER 176 (Oxford Univ. Press 2018).

[12] *Id.* at 176.

[13] *See* U.N. OFF. ON DRUGS & CRIME, CURRENT PRACTICES IN ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF SERIOUS AND ORGANIZED CRIME, U.N. Sales No. E.09.XI.19 (2009) (describing electronic surveillance tools employed by governments in investigating serious and organized crime); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. R. 62, 65–66 (2013); DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 46 (Cambridge Univ. Press 2017). See generally SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING (Oxford Univ. Press 2020) for an excellent, in-depth overview of how different forms of government surveillance fit together.

[14] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 216 (2007).

[15] NEIL RICHARDS, WHY PRIVACY MATTERS 72 (2022).

[16] *Id.* at 72–78.

[17] Priscilla M. Regan, *Legislating Privacy*, *in* SURVEILLANCE STUDIES: A READER 213, 216 (Torin Monahan & David Murakami Wood eds., 2018).

[18] SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS, 104–05 (2021).

fundamental level, privacy is necessary to develop as a person. So the loss of privacy in the face of government surveillance comes at a cost.[19]

More importantly, the threat and cost of surveillance does not fall on our society equally.[20] As Skinner-Thompson masterfully articulated in his recent book, *Privacy at the Margins*, "[M]arginalized communities experience less lived privacy, are subject to greater degrees of surveillance, and feel the burdens of any surveillance more acutely."[21] Marginalized communities include those who are economically disadvantaged,[22] racial minorities,[23] religious minorities,[24] queer communities,[25] women,[26] and others. Moreover, surveillance increases contact with the criminal justice system.[27] Every year, law enforcement in the United States kills around 1,000 civilians. Black men are two and a half times more likely than white men to be fall in that category.[28] Privacy stakes for these communities cannot be overstated.

This brief description of modern law enforcement surveillance and its costs are by no means exhaustive. It merely establishes that there are legitimate concerns surrounding modern surveillance, which courts have recently begun to address.[29]

In the context of the Fourth Amendment, the adoption of the surveillance technologies and techniques discussed above has led to what Margot Kaminski refers to as the "disruption of the 'imagined regulatory scene'"[30] Quoting the work of Jack Balkin

---

[19] *See, e.g.,* SLOBOGIN, *supra* note 14, at 92–98; GRAY, FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, *supra* note 13, at 8–14.

[20] *See* SKINNER-THOMPSON, *supra* note 18.

[21] *Id.* at 16.

[22] *Id.* at 17.

[23] *Id.* at 25.

[24] *Id.* at 28.

[25] *Id.* at 29.

[26] *Id.* at 39.

[27] *See* Sarah Brayne, *Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment*, 79 AM. SOCIO. REV. 367, 367 (2014).

[28] Lynne Peeples, *What the data say about police brutality and racial bias—and which reforms might work*, NATURE (June 19, 2020), https://nature.com/articles/d41586-020-01846-z.

[29] *See* Citron & Gray, *supra* note 10, at 389–90 (explaining how courts may be posed "to decide whether the Fourth Amendment might impose some restraint on the use of modern surveillance technologies by law enforcement officers and their private-sector proxies.").

[30] Margot E. Kaminski, *Technological "Disruption" of the Law's Imagined Scene: Some Lessons from Lex Informatica*, 36 BERKELEY TECH. L. J. 883, 895 (2022) (quoting Jack M. Balkin & Reva B. Siegel, *Principles, Practices, and*

and Reva Siegel, Kaminski reiterates the principles underlying the imagined regulatory scene, noting:

> [L]egal principles are intelligible and normatively authoritative only insofar as they presuppose a set of background understandings about the paradigmatic cases, practices, and areas of social life to which they properly apply. A principle always comes with an *imagined regulatory scene* that makes the meaning of the principle coherent to us.[31]

Kaminski explains that technology can disrupt the imagined regulatory scene "not by departing from the [imagined paradigmatic scenario] entirely, but by constraining, enabling, or mediating behavior, both by actors we want the law to constrain and actors we want the law to protect."[32] This disruption then "upset[s] some 'balance' within the imagined scene that serves a legal principle," which "can threaten a legal principle or cause us to reexamine it."[33] Kaminski connects her ideas specifically to the Fourth Amendment and identifies Orin Kerr's equilibrium adjustment theory as an example of a response to the disruption of the imagined regulatory scene.[34]

For his equilibrium adjustment theory, Kerr sets up a hypothetical "Year Zero" where there are "no tools to help commit or investigate crimes."[35] According to Kerr, applying the Fourth Amendment would be easy because "[i]n this simple world of Year Zero, criminal investigations would employ only a handful of basic steps to find evidence, seize it, and use it to prove cases beyond a reasonable doubt in court."[36] At "Year Zero," the Fourth Amendment "strikes a balance of police power," leading to rules that grant the government "some powers to enforce the law" as well as to rules restricting the government's ability to abuse their powers.[37] But the advent and adoption of new technologies can throw off this equilibrium.[38] When this occurs, or "[w]hen judges perceive that changing technology . . . significantly enhances government power, courts embrace higher protections to counter

---

Social Movements, 154 U. PA. L. REV. 927, 928 (2006)).

[31] Kaminski, *supra* note 30, at 896 (quoting Balkin & Siegel, *supra* note 30, at 928) (alteration in original).

[32] *Id.* at 898.

[33] *Id.* at 903.

[34] *Id.* at 907 (citing Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 484 (2011)).

[35] Kerr, *supra* note 34, at 482.

[36] *Id.* 483.

[37] *Id.* 485.

[38] *Id.* 485–86.

the expansion of government power."[39]

The mosaic theory represents one way that courts have tried to respond to the disrupted imagined regulatory scene and restore equilibrium in the face of modern surveillance techniques.[40] The mosaic theory "considers whether a set of non-searches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic."[41] This contrasts with the sequential analysis, which is the traditional form of Fourth Amendment analysis that defines a search by "ask[ing] if the government's conduct has crossed the boundary from outside to inside surveillance."[42] Unlike the mosaic theory, which aggregates government conduct, the sequential approach analyzes government conduct "frame by frame" to determine if any individual government action constitutes a search.[43] To understand the shift from the sequential approach to the mosaic theory, and how that shift fits under the equilibrium adjustment theory, a brief review of the mosaic theory's adoption is necessary.[44]

The mosaic theory began with a 2010 D.C. Circuit case, *United States v. Maynard*,[45] which the Supreme Court reviewed in 2012 as *United States v. Jones*.[46] In *Maynard*/*Jones*, law enforcement installed a GPS tracker on Jones's car and used it to track his location for twenty-eight days.[47] Although law enforcement had a

---

[39] Kerr, *supra* note 34, at 487–88.

[40] Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012) ("The mosaic approach is animated by legitimate concerns: it aims to maintain the balance of Fourth Amendment protection as technology changes, a method I have elsewhere called 'equilibrium-adjustment.'").

[41] *Id.* at 320. *See also* GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, *supra* note 13, at 109 ("The fundamental insight behind the mosaic theory is that we can maintain reasonable expectations of Fourth Amendment privacy in certain quantities of information and data even if we lack a reasonable expectation of privacy in the constituent parts of that whole.").

[42] Kerr, *supra* note 40, at 317.

[43] *See id.*

[44] The history of the mosaic theory has been previously discussed at length, so this Note provides only a brief summary for context. See Kerr, *supra* note 40, and Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, S. CT. REV. 205, 205–08 (2015), for a pre-*Carpenter* history. See ORIN KERR, *IMPLEMENTING CARPENTER*, THE DIGITAL FOURTH AMENDMENT (forthcoming) for a post-*Carpenter* discussion.

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

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

[47] *See id.* at 402–03.

warrant to install the GPS tracker, they did not comply with the terms of that warrant.[48] Jones subsequently filed a motion to suppress the evidence from the GPS tracker at his trial, where he faced conspiracy charges related to drug distribution.[49] The district court granted his motion in part, suppressing the GPS evidence from when his car was parked in his garage, but allowed the rest, holding that under *Knotts*,[50] Jones had no reasonable expectation of privacy when driving in public.[51]

The D.C. Circuit reversed, holding that *Knotts* did not control because there was a difference "between the limited information discovered by use of the beeper—movements during a discrete journey—and more comprehensive or sustained monitoring."[52] Thus, the D.C. Circuit held that the extended use of GPS tracking violated a reasonable expectation of privacy, even though it occurred in publicly viewable areas where the police or anyone else could freely follow Jones, because "the whole may be more revealing than the parts."[53] Referring to the "mosaic theory" as used in the national security context, the D.C. Circuit explained:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[54]

According to Kerr, the D.C. Circuit's approach "redefined the basic unit of Fourth Amendment law" by asking not whether

---

[48] *See Jones*, 565 U.S. at 403, n.1.
[49] *See id.* at 403.
[50] United States v. Knotts, 460 U.S. 276 (1983).
[51] *See Jones*, 565 U.S. at 403.
[52] *See* United States v. Maynard, 615 F.3d 555–56 (D.C. Cir. 2010).
[53] *See id.* at 561.
[54] *Id.* at 562 (footnote omitted).

"discrete pieces of GPS information" violated a reasonable expectation of privacy, but instead "whether the entirety of the GPS monitoring over the course of twenty-eight days, *considered as a collective whole*" violated a reasonable expectation of privacy.[55]

The Supreme Court affirmed the D.C. Circuit under the trespass theory of the Fourth Amendment,[56] but concurring opinions by Justice Sotomayor[57] and Justice Alito joined by Justices Ginsburg, Breyer, and Kagan,[58] employed mosaic theory reasoning. Justice Sotomayor, concerned that "[a]wareness that the government may be watching chills associational and expressive freedoms," explained that "when considering the existence of a reasonable societal expectation of privacy in the *sum* of one's public movements," the question should be "whether people reasonably expect that their movements will be recorded and *aggregated* in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[59] Justice Alito, alternatively, focused not on what law enforcement could learn, but on society's expectations, concluding that while short-term GPS monitoring might be expected, long-term monitoring was not expected because "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period."[60] Although their approaches varied, both Justice Sotomayor and Justice Alito used a variant of the mosaic theory by "analyz[ing] the collective sum of government action, rather than individual sequential steps," to evaluate whether government conduct constituted a Fourth Amendment search.[61]

Six years later, in *Carpenter v. United States*, the Supreme Court potentially adopted the mosaic theory.[62] At trial, the government used historical cell-site location information ("CSLI") to place Carpenter, the suspect in a series of robberies, near the location of four of these crimes at the time that the robberies took

---

[55] Kerr, *supra* note 40, at 324.
[56] *Jones*, 565 U.S. at 404–05.
[57] *See id.* at 413 (Sotomayor, J., concurring).
[58] *See id.* at 418 (Alito, J., concurring).
[59] *Id.* at 416 (Sotomayor, J., concurring) (emphasis added).
[60] *Id.* at 430 (Alito, J., concurring).
[61] *See* Kerr, *supra* note 40, at 328.
[62] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

place.[63] Law enforcement had obtained a subpoena under the Stored Communications Act for the CSLI records but failed to secure a warrant.[64] Carpenter sought to suppress the CSLI evidence, claiming his Fourth Amendment rights were violated because the acquisition of the CSLI was a warrantless search.[65] The Court agreed, holding that Carpenter's Fourth Amendment rights were violated because the acquisition of the CSLI constituted a warrantless search under the Fourth Amendment.[66]

The Court first explained its recent application of equilibrium adjustment when addressing "innovations in surveillance tools," noting that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure . . . preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[67] Turning specifically to historical CSLI, the Court echoed Justice Sotomayor's *Jones* concurrence, recognizing that the extensive tracking offered by historical CSLI amounted to knowledge of "the whole of [an individual's] physical movements."[68] Such knowledge "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[69] Stressing the pervasiveness of cellphones, the Court explained:

> Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.[70]

Despite the Court's concern over law enforcement's use of historical CSLI, the Court did not apply the sequential approach.[71] Thus, they did not hold that the use of *any* CSLI was

---

[63] *Carpenter*, 138 S. Ct. at 2213.
[64] *Id.* at 2212.
[65] *Id.*
[66] *Id.* at 2220.
[67] *Id.* at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)) (alteration in original).
[68] *See id.* at 2217–19 (internal citations omitted).
[69] *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J. concurring)).
[70] *Id.*
[71] *Id.*

a search.[72] Instead, the Court held that it "need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[73] In suggesting that there could be a difference between the short-term (some amount less than seven days) and long-term (seven or more days) use of historical CSLI, the Court seemed to use mosaic reasoning.[74] Further complicating the Court's rather equivocal adoption of the mosaic theory, the Court went on to stress that the holding of *Carpenter* was a "narrow one."[75] It noted that it was not ruling on the use of real-time CSLI nor "call[ing] into question conventional surveillance techniques and tools."[76]

Since *Carpenter*, lower courts have struggled to figure out what to do with the mosaic theory.[77] Indeed, the courts are split on whether the Supreme Court adopted the mosaic theory at all.[78] One Florida court explicitly stated that "[t]he decision in *Carpenter* does not address the 'mosaic' theory."[79] But a Massachusetts court expressly applied the mosaic theory, believing that *Carpenter* "articulated an aggregation principle for the technological surveillance of public conduct, sometimes referred to as the mosaic theory."[80] When courts decide to apply the mosaic theory to a given technology, they face a dizzying

---

[72] *Carpenter*, 138 S. Ct. at 2217 (emphasis added).

[73] *Id.* at 2217, n.3.

[74] *See* Kerr, *supra* note 40, at 333–36 (describing applicability of mosaic theory in judicial reasoning requires, *inter alia*, an assessment of the duration and scale the surveillance tool used).

[75] *Carpenter*, 138 S. Ct. 2220.

[76] *Id.*

[77] Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter*, 26 BERKELEY J. CRIM. L. 71, 107–08 (2021); *see also* Taylor H. Wilson, Jr., *The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts*, 99 TEX. L. REV. ONLINE 155, 156 (2021) ("*Carpenter*'s shift has led to confusion about the place of the 'mosaic theory' in Fourth Amendment doctrine.").

[78] Fairbanks, *supra* note 77, at 107–08.

[79] Bailey v. State, 311 So. 3d 303, 312 n.6 (Fla. Dist. Ct. App. 2020), *rev. denied*, Case No. SC21-382, 2021 WL 2408431 (Fla. 2021), *cert. denied*, 142 S. Ct. 568 (2021).

[80] Commonwealth v. McCarthy, 142 N.E.3d 1090, 1102–03 (Mass. 2020) (footnote omitted).

array of issues with no clear answers.[81] Many of these issues, and the surveillance concerns that spurred them, are exemplified in a recent Fourth Circuit case, *Leaders of a Beautiful Struggle v. Baltimore Police Department*.[82]

PART II:

Leaders of a Beautiful Struggle serves as a case study for both the powerfully invasive surveillance tools used by law enforcement and the difficulties the judiciary faces in responding to the threats posed by those tools.[83] This Part begins by reviewing the facts of the case, focusing on law enforcement's ability to surveil the entirety of Baltimore. Next, this Part summarizes the various opinions of the courts—the district court, the Fourth Circuit panel, and the Fourth Circuit sitting *en banc*—exploring the judges' attempts to apply the Fourth Amendment to city-wide aerial surveillance. Finally, this Part addresses takeaways from the Fourth Circuit's application of the mosaic theory, concluding that even though the court protected privacy, the mosaic theory remains a poor answer to a serious problem.

A. Leaders of a Beautiful Struggle: The Facts

In *Leaders of a Beautiful Struggle*, a group of Baltimore community advocates sought to enjoin the Baltimore Police Department ("BPD") from implementing its Aerial Investigation Research ("AIR") program.[84] The AIR program was a complex surveillance scheme, involving a partnership between the BPD and the aptly named Persistent Surveillance Systems, a private contractor.[85] Under the AIR program, multiple planes would fly over Baltimore during daylight hours, each logging air time of at least forty hours a week.[86] The planes were equipped with "Hawkeye Wide Area Imaging System" camera technology.[87] "The cameras captur[ed] roughly 32 square miles per image per

---

[81] Kerr, *supra* note 40, at 313–15; Fairbanks, *supra* note 77, at 108–11.

[82] *See generally* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021).

[83] *See id.*

[84] *Id.* at 333.

[85] *Id.*

[86] *Id.* at 334.

[87] *Id.*

second."[88] Each image could be magnified such that individual people and cars were visible as "blurred dots or blobs."[89] On average, the AIR planes "obtain[ed] an estimated twelve hours of coverage of around 90% of the city each day, weather permitting."[90]

The images were transmitted "to PSS 'ground stations' where contractors use[d] the data to 'track individuals and vehicles from a crime scene and extract[ed] information to assist BPD in the investigation of Target Crimes."[91] This information would be assembled into "reports" and "briefings" that were supplied to BPD officers on the case.[92] To create these reports, PSS contractors integrated the images into other BPD surveillance systems, including BPD's dispatch system, "CitiWatch" security cameras, "Shot Spotter" gunshot detection, and license plate readers.[93] This allowed the contractors to include:

> from both before and after the crime: 'observations of driving patterns and driving behaviors'; the 'tracks' of vehicles and people present at the scene; the locations those vehicles and people visited; and, eventually, the tracks of the people whom those people met with and the locations they came from and went to.[94]

AIR data was stored on PSS's servers for forty-five days.[95] PSS maintained the reports and related images "indefinitely as necessary for legal proceedings and until relevant statutes of limitations expire."[96]

B. The District Court Opinion

The district court performed a traditional Fourth Amendment analysis and found that using the AIR program did not constitute a search.[97] The district court began this analysis by reviewing Fourth Amendment aerial surveillance jurisprudence,[98] including

---

[88] *Leaders of a Beautiful Struggle*, 2 F.4th at 334
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 717 (D. Md. 2020), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *reh'g en banc granted*, 831 F. App'x 662 (4th Cir. 2020), *and on reh'g en banc*, 2 F.4th 330 (4th Cir. 2021), *and rev'd and remanded*, 2 F.4th 330 (4th Cir. 2021).
[98] *Id.* at 712.

Dow Chemical Co. v. United States, *California v. Ciraolo*, and *Florida v. Riley*, as well as Fourth Circuit precedent.[99] Based on that case law, the district court concluded that "[t]he AIR pilot program is far less invasive than the feats of aerial surveillance permitted" in previous Fourth Amendment aerial surveillance cases.[100] Next, the Court analogized to pole cameras, noting that "numerous" federal Courts of Appeals upheld the warrantless use of pole cameras.[101] The court explained that pole cameras are a "highly invasive means of surveillance, capable of observing a person's facial features and bodily movements as they navigate their habitual environs."[102] The court noted that "[e]ven when fully integrated with existing BPD surveillance tools, the AIR pilot program could not capture a host of private activities ordinarily subject to pole camera surveillance."[103] Because more invasive aerial surveillance and pole cameras were permitted without warrants, the court concluded that the AIR program was similarly permissible.[104]

Finally, the district court rejected the plaintiffs' argument that *Carpenter* applied to the AIR program.[105] The court recognized that the *Carpenter* holding was "narrow" and "did not 'call into question conventional surveillance techniques and tools, such as security cameras.'"[106] Unlike the CSLI at issue in *Carpenter*, the AIR pilot program could not continuously track the "whole of [the plaintiffs'] physical movements."[107] The AIR program also did not run at night or during inclement weather, and had coverage gaps that prohibited continuous tracking, which was not true for CSLI.[108] AIR tracking was also more time intensive than CSLI tracking,[109] and the AIR program could only track in public places.[110] CSLI, alternatively, could find an individual anywhere.[111]

---

[99] *Leaders of a Beautiful Struggle*, 456 F. Supp. 3d at 713.
[100] *Id.* at 713–14.
[101] *Id.* at 714.
[102] *Id.* (citing United States v. Vankesteren, 553, F.3d 286, 291 (4th Cir. 2009).
[103] *Id.*
[104] *Id.* at 712–14.
[105] *Id.* at 715–16.
[106] *Id.* at 715 (citing Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018)).
[107] *Id.* at 716.
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*

Importantly, to support its conclusion that the AIR program did not provide as much information as CSLI, the court held that "seeking to lump together discrete surveillance activities as one Fourth Amendment 'search,' is simply without merit."[112] The court explained:

> Using a combination of resources and activities—including police interviews, CitiWatch cameras, license plate readers, and public records—the Baltimore Police Department may be able to reconstruct a detailed account of a person's activities and associations. The addition of one more investigative tool—in this case, aerial surveillance—does not render the total investigatory effort a Fourth Amendment "search." In *Carpenter*, the Supreme Court focused on the acquisition of CSLI and its extraordinary qualities; it did not draw significant attention to ancillary investigative tools used to corroborate or interpret information obtained through CSLI. Accordingly, *Carpenter* does not grant license to define a Fourth Amendment "search" so broadly that it encompasses several steps in the total investigatory effort.[113]

This reasoning was ultimately rejected by the Fourth Circuit sitting *en banc*, and when combined with a mosaic theory, led the Fourth Circuit to the opposite conclusion.[114]

C. Fourth Circuit Court of Appeals Panel Opinion

The Fourth Circuit panel largely adopted the district court's reasoning and held that the AIR program was not a search.[115] Relying on many of the same cases as the district court, the panel emphasized "that an individual has a limited expectations of privacy in his or her public movements."[116] But the panel went further than the district court to distinguish the AIR program from *Carpenter* and *Maynard/Jones*, using the mosaic theory to differentiate between what it viewed as short-term surveillance and long-term surveillance.[117]

The court explained,

---

[112] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 716 (D. Md. 2020).

[113] *Id.* at 716–17.

[114] *See Leaders of a Beautiful Struggle*, 2 F.4th at 334.

[115] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 979 F.3d 219, 232 (4th Cir. 2020), *reh'g en banc granted*, 831 F. App'x 662 (2020), *and on reh'g en banc*, 2 F.4th 330 (4th Cir. 2021). The court also applied a balancing test based on public safety problems, coming to the same conclusion as the regular reasonable expectation of privacy test. *See id.*

[116] *Id.* at 227.

[117] *Id.* at 227–29.

> *[S]hort-term* surveillance of an individual's *public* movements is less likely to violate a reasonable expectation of privacy. And under that rule, the AIR program passes muster. As Judge Bennett explained, the built-in limitations of the AIR program mean that it *only* enables the short-term tracking of public movements. First, the AIR program's cameras are only able to track outdoor movements. They cannot track an individual who enters a building, and analysts cannot tell if the person leaving the building is the same person who entered it. Second, AIR's surveillance planes only fly during twelve daylight hours. Because they do not fly at night, AIR surveillance cannot be used to track individuals from day-to-day.[118]

Just as with the district court, the panel noted that day-to-day tracking could occur if the AIR program was used "in conjunction" with other surveillance tools, but that those tools were not being challenged as searches.[119] Thus, only the AIR program's independent capabilities needed to be considered.[120] Further exemplifying its application of the mosaic theory, the panel cautioned that its "opinion should not be overread."[121] It explained that more extensive aerial surveillance, such as twenty-four-hour surveillance, may implicate the Fourth Amendment.[122] By repeatedly distinguishing between short and long-term surveillance, the panel squarely adopted mosaic theory reasoning to hold that the AIR program did not constitute a search.[123]

Tellingly, even though the panel found that the AIR program was permissible, it demonstrated awareness of the concerns and dangers of surveillance.[124] In addition to stating that its opinion should not be overread and a more extensive program could be judged differently, the panel made clear that it did not believe the Supreme Court "issued sweeping approvals of suspicionless search programs."[125] The panel explicitly recognized that while "[r]apid advancements in technology hold real promise in preventing and resolving crimes," they also "pose unprecedented

---

[118] *Leaders of a Beautiful Struggle*, 979 F.3d at 227.
[119] *Id.*
[120] *See id.*
[121] *Id.* at 229.
[122] *Id.*
[123] *See id.* at 234–35 (Gregory, J., dissenting). In his dissent, Judge Gregory came to the opposite conclusion. *Id.* Because he wrote the *en banc* majority, this Part does not address his dissent.
[124] *See id.* at 229.
[125] *Id.* at 230.

threats to personal privacy."[126] But in this case, even though "there are aerial surveillance programs that would transgress basic Fourth Amendment protections," the AIR program did not cross the line.[127]

D. The Fourth Circuit En Banc Opinion

In an opinion authored by Chief Judge Roger Gregory, the Fourth Circuit, sitting *en banc*, reversed the panel, holding that accessing AIR program data was a Fourth Amendment search and that "*Carpenter* applie[d] squarely to this case."[128] Applying the mosaic theory, the *en banc* court explained that "*Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns."[129] Unlike the panel and district court, the majority held that the AIR program surveillance "'tracks every movement' of every person outside in Baltimore" and could therefore reveal the intimate details protected by *Carpenter*.[130]

To address the panel and district court's opinions, the majority found that though there were gaps in surveillance because the planes flew in twelve-hour increments, the AIR program nevertheless constituted long-term surveillance because it enabled the government to track location, through photographs, in "multi-hour" blocks over the course of "consecutive days" for a month and a half.[131] The *en banc* court further highlighted that the surveillance in *Carpenter* and *Jones* had gaps, but that the Supreme Court nonetheless found "in both cases, the surveillance still surpassed ordinary expectations of law enforcement's capacity and provided enough information to deduce details from the whole of individuals' movements."[132] Discussing how the AIR program could reveal the whole of individuals' movements, the court explained:

AIR data is a photographic record of movements, surpassing the

---

[126] *Leaders of a Beautiful Struggle*, 979 F.3d at 231–32 (Gregory, J., dissenting).

[127] *Id.* at 232.

[128] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333 (4th Cir. 2021).

[129] *Id.* at 341.

[130] *Id.*

[131] *Id.* at 342–43.

[132] *Id.* at 343.

> precision even of GPS data and CSLI, which record variable location points from which movements can be reconstructed. And while the coverage is not 24/7, most people do most of their moving during the daytime, not overnight. Likewise, many people start and end most days at home, following a relatively habitual pattern in between. These habits, analyzed with other available information, will often be enough for law enforcement to deduce the people behind the pixels. And if a track is interrupted by sunset, police will at least sometimes be able to re-identify the same target over consecutive days. For example, law enforcement could use AIR data to track a person's movements from a crime scene to, eventually, a residential location where the person remains. They could then look through time and track movements from that residence. They could use any number of context clues to distinguish individuals and deduce identity. After all, the AIR program's express goal is to identify suspects and witnesses to help BPD solve crimes.[133]

Thus, the *en banc* majority again disagreed with the panel and district court, noting that the AIR program's reliance on integrating other surveillance systems did not change any Fourth Amendment calculus.[134] The majority emphasized that the focus of a Fourth Amendment analysis is not just "raw data," but rather "what that data can reveal."[135] Because AIR program data "enable[d] deductions from the whole of individuals' movements," it revealed more than "short-term" information and was not "mere[ly]" an "augmentation of ordinary police capabilities."[136]

The *en banc* majority drew three dissents, the most significant of which was Judge Wilkinson's dissent.[137] The Wilkinson dissent was joined in full by Judges Niemeyer, Agee, and Quattlebaum and joined in part by Judges Diaz, Richardson, and Rushing.[138] Judge Wilkinson believed that "the majority engage[d] in an indefensible exercise of judicial overreach" because local officials should have "leeway to experiment" when they design and implement surveillance programs based on "new technology."[139] Offering a classic separation of powers argument, Judge Wilkinson urged deference to elected officials, stressing that courts are not well-positioned to deal with rapidly changing

---

[133] *Leaders of a Beautiful Struggle*, 2 F.4th at 343.
[134] *Id.* at 344.
[135] *Id.*
[136] *Id.* at 345.
[137] *See id.* at 351–69 (Wilkinson, J., dissenting).
[138] *See id.*
[139] *Id.* at 355, 359.

technologies, particularly when balancing between the need for public safety with the need for privacy.[140]

Judge Wilkinson also took issue with the majority's doctrinal analysis, citing the same cases as the panel and the district court, stating that the AIR program was short-term aerial surveillance and thus permissible.[141] To support that conclusion, he distinguished *Carpenter*, explaining that CSLI is "far more invasive of privacy than the limited aerial surveillance in this case."[142] Wilkinson further took issue with the majority's failure to view the AIR program in a "programmatic context[]."[143] In that context, courts should use a balancing test to measure "the asserted burdens on constitutional rights against the claim of law enforcement and public safety needs."[144]

Finally, Judge Wilkinson addressed broader privacy policy concerns. He claimed that while "the majority may think it is striking a great blow in the name of privacy," the *en banc* majority decision may in fact inadvertently push cities to adopt more invasive surveillance measures.[145] In Wilkinson's view, cities like Baltimore must do something to deal with rising violent crime rates.[146] Thus, if programs like AIR are found constitutionally impermissible, Baltimore and other cities may rely instead on more traditional surveillance measures such as ground surveillance cameras.[147] These traditional programs, Judge Wilkinson argued, "may well pose a more pervasive threat to privacy than AIR."[148] Ultimately, Judge Wilkinson concluded that the majority's "precipitous and gratuitous ruling will contribute to the continuation of a great human tragedy," and that "surely Fourth Amendment reasonableness does not conscript [the court] in an effort to deny cities the right to find answers, to discover what works for them."[149]

In a separate concurrence, Chief Judge Gregory, joined by Judges Wynn, Thacker, and Harris, acknowledged the violence facing Baltimore but argued that the dissent was wrong to

---

[140] *Leaders of a Beautiful Struggle*, 2 F.4th at 359 (Wilkinson, J., dissenting).
[141] *Id.* at 362.
[142] *Id.* at 361.
[143] *Id.* at 362.
[144] *Id.* at 361–62.
[145] *Id.* at 364–65.
[146] *Id.* at 365.
[147] *Id.*
[148] *Id.*
[149] *Id.* at 368–69.

"take[] for granted" that policing should be "the antidote to killing."[150] Squarely addressing the social justice issues that often accompany policing and surveillance concerns, Chief Judge Gregory highlighted "the systems, relationships, and foundational problems that have perpetuated Baltimore's epidemic of violence" to explain that the AIR program is not "so obviously a lifeline."[151] Gregory cited Judge Wynn's concurrence to explain that "Black neighborhoods in Baltimore are already disproportionately policed."[152]

Judge Wynn, joined by Judges Motz, Thacker, and Harris, went even further to address policing and surveillance as solutions to violence.[153] In an extensive footnote, Judge Wynn explained that Baltimore was "over policed," "under policed," and "just plain *poorly* policed."[154] In support of each of these assertions, Judge Wynn provided a bevy of sources that documented the impact that race and class played in determining who bore the brunt of the consequences of Baltimore's policing problems.[155]

E. Lessons from Leaders of a Beautiful Struggle

The facts of *Leaders of a Beautiful Struggle* demonstrate the modern capabilities of government surveillance. While aerial surveillance has been around for a long time, the AIR program was different both in degree and in kind.[156] Modern technology allowed the AIR planes to be in the air longer and obtain greater numbers of images than was previously possible.[157] Similarly, modern computers allowed police to integrate the captured images with other new surveillance techniques, such as automatic license plate readers.[158] Altogether, the AIR program was a newly possible form of dragnet surveillance that captured

---

[150] *Leaders of a Beautiful Struggle*, 2 F.4th at 348 (Wilkinson, J., dissenting).
[151] *Id.* at 349.
[152] *Id.*
[153] *Id.* at 350–51.
[154] *Id.* at 350 n.*.
[155] *Id.*
[156] Greg Nojeim, *Court Rules that Warrantless Persistent Aerial Surveillance Is Unconstitutional*, CNTR. FOR DEMOCRACY & TECH. (July 19, 2021), https://cdt.org/insights/court-rules-that-warrantless-persistent-aerial-surveillance-is-unconstitutional.
[157] Andrew R. Morral et al., *Evaluating Baltimore's Aerial Investigation Research Pilot Program: Interim Report*, RAND CORP. 8 (2021), https://doi.org/10.7249/RRA1131-2.
[158] *Id.*

everyone in an entire city.[159] For almost all of human history, this scale of surveillance would have been impossible.[160] But given the capabilities of modern technology, the AIR program was exactly the sort of government surveillance technique the implicates the concerns raised in Part I.[161] So while it is understandable that the Fourth Circuit felt compelled to act to protect privacy interests, their use of the mosaic theory to try and fit Fourth Amendment protection to this sort of dragnet surveillance technique was misguided.

Leaders of a Beautiful Struggle does an excellent job of exemplifying the issues with the mosaic theory.[162] As a preliminary matter, at least in the district court's opinion, there was doubt as to whether *Carpenter* and the mosaic theory should even apply to the facts of *Leaders*.[163] Once the Fourth Circuit decided to apply the mosaic theory, it split on how to do so.[164] It struggled to answer questions such as how much surveillance was too much, or even more fundamentally, how to properly measure the amount of surveillance actually occurring.[165] That surveillance may have been twelve hours or the total number of days the program existed, but with either measure, it was unclear how the gaps in coverage should factor in.[166] Another complicating factor was how to evaluate the integration of the AIR system with other surveillance systems.[167] If integration was a major issue, then which precise part of the AIR system constitutes a search? The taking of photographs themselves? Or

---

[159] *See* Morral et al., *supra* note 157 (stating that the "camera equipped aircraft were intended to fly in designated orbits above the city" in four different 30 square mile zones, which would allow the "capture of imagery for most of the more densely populated areas of the city").

[160] Kien Nguyen et al., *The State of Aerial Surveillance: A Survey*, CORNELL UNIV. (2022) (available at http://cvlab.cse.msu.edu/pdfs/Nguyen_Fookes_Sridharan_Tian_Liu_Liu_Ross_AerialSurveillance.pdf).

[161] *See supra* Part I.

[162] Scott A. Havener, *Leaders of a Beautiful Struggle v. Baltimore Police Department: The Fourth Amendment Continues Its Struggle to Make Sense of the Twenty-First Century*, 68 LOY. L. REV. 159, 177 (2021).

[163] Leaders of a Beautiful Struggle v. Balt. Police Dep't., 456 F. Supp. 3d 699, 715–17 (D. Md. 2020) (discussing the application of *Carpenter* to the facts of the case).

[164] Fairbanks, *supra* note 77, at 93–94.

[165] *See id.* at 110.

[166] Wilson, *supra* note 77, at 175.

[167] *See* Orin Kerr (@OrinKerr), TWITTER (June 24, 2021, 2:06 PM), https://twitter.com/OrinKerr/status/1408124404341657602 ("The court is also influenced by the ability to combine this information with other information.") (Which I would think is true of all information-gathering, but so it goes.)).

law enforcement's access of them?

Some of the complexities of the case undoubtedly come from its procedural posture. Rather than a criminal defendant who challenges the use of evidence at trial, the *Leaders of a Beautiful Struggle* plaintiffs were concerned citizens seeking to enjoin an entire program.[168] In the former, a court would be asked to evaluate a determinate amount of GPS evidence, as in *Jones*, or a set number of days of CSLI, as in *Carpenter*.[169] But in *Leaders*, the court was asked to grapple with the same issues abstractly, based on the structure but not specific uses of the AIR program.[170] It is clear from how the three *Leaders* opinions grappled with those issues that, at least in the abstract, there is no easy answer under the Fourth Amendment.[171]

This is in part because the imagined regulatory scene has been disturbed to such an extent that equilibrium adjustment under the Fourth Amendment alone cannot address modern dragnet government surveillance.[172] As Justice Alito humorously pointed out in his *Jones* concurrence, when it came to multi-day GPS tracking, "it is almost impossible to think of late-18th-century situations that are analogous" unless there was a "very tiny constable . . . with incredible fortitude and patience" who could hide somewhere in a coach like a human GPS.[173] Applying that idea to this case is even more preposterous—the government would need hundreds of thousands of pocket-sized constables to follow Baltimore's residents.[174] Those pocket-sized constables would need to constantly send each other letters, comparing the movements of their assigned residents. Someone would then need to compile those letters and movements into a format very dedicated investigators would later sort through manually.

It is possible to interpret this awkward historical comparison to indicate that Fourth Amendment analyses never should have been applied to facts like those in *Leaders* or *Carpenter* in the first place. Justice Thomas suggested as much in his *Carpenter*

---

168 *Leaders of a Beautiful Struggle*, 2 F.4th at 333.

169 *See* United States v. Jones, 565 U.S. 400, 402 (2012); Carpenter v. United States, 138 S. Ct. 2206, 2208 (2018).

170 *Leaders of a Beautiful Struggle*, 2 F.4th at 337.

171 *Id.* at 342.

172 *Id.* at 348–49.

173 *Jones*, 565 U.S. at 420 n.3 (Alito, J., concurring).

174 *QuickFacts: Baltimore City, Maryland, United States*, U.S. CENSUS BUREAU, https://census.gov/quickfacts/fact/table/baltimorecitymaryland,US/PST045219 (last visited Feb. 6, 2022).

dissent, claiming "the reasonable expectation of privacy test . . . has no basis in the text or history of the Fourth Amendment."[175] He believed that "[u]ntil we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence."[176] The Fourth Amendment, Justice Thomas argued, was meant to be limited to physical security and property, which are interests not implicated by something like the AIR program.[177] Justice Gorsuch echoed similar concerns:

> [T]he [Fourth] Amendment's protections do not depend on the breach of some abstract 'expectation of privacy' whose contours are left to the judicial imagination. Much more concretely, it protects your "person," and your "houses, papers, and effects." Nor does your right to bring a Fourth Amendment claim depend on whether a judge happens to agree that your subjective expectation to privacy is a "reasonable" one. Under its plain terms, the Amendment grants you the right to invoke its guarantees whenever one of your protected things . . . is unreasonably searched or seized. Period.

If Justices Thomas and Gorsuch are correct, the Fourth Amendment is not meant to apply to dragnet government surveillance at issue here, and the question whether it applies exists only because Fourth Amendment analysis has been severely distorted. That is why it is hard for courts to address their very legitimate surveillance concerns; their only real tool, the Fourth Amendment, simply does not fit.

But the *Carpenter* majority maintained the *Katz* reasonable expectation test,[178] and Kerr, "one of the nation's leading Fourth Amendment scholars,"[179] argues that *Katz* can be understood through an originalist lens that "accurately tracks the constitutional text and reflects a sound interpretation of its original public meaning."[180] If that is true, it is less obvious that the Fourth Amendment can't solve the issues presented by dragnet government surveillance like the AIR program. But the issues and questions raised by *Leaders of a Beautiful Struggle* are telling. As Kerr Tweeted in describing the *en banc* opinion, "I

---

[175] Carpenter v. United States, 138 S. Ct. 2206, 2236 (2018) (Thomas, J., dissenting).

[176] *Id.*

[177] *See id.* at 2238–41 (Thomas, J., dissenting).

[178] *Id.* at 2217.

[179] United States v. Howard, 426 F. Supp. 3d 1247, 1256 n.7 (M.D. Ala. 2019), *aff'd*, 858 F. App'x 331 (11th Cir. 2021).

[180] Orin Kerr, *Katz as Originalism*, 71 DUKE L. J. 1047, 1047 (2022).

am kind of amazed that this sort of reasoning is in the name of the 4th Amendment, as it seems so far 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."[181] He suggested that the issue is the mosaic theory, but there is no clear alternative to get Fourth Amendment protection against AIR-type surveillance.

Due to a variety of longstanding Fourth Amendment doctrines,[182] as the district court pointed out, traditional Fourth Amendment analysis likely leaves the AIR program undisturbed and thus offers no help.[183] Kerr provides an alternative to both the mosaic theory (and its plethora of issues) and traditional Fourth Amendment analyses. He calls this alternative the "Source Rule."[184] "Under the Source Rule, government access to any information that owes its source to *Carpenter*-protected information is a search."[185] But the Source Rule would likely not apply to the AIR program. In Kerr's view, "Pre-digital records and their modern equivalents are exempt, sort of like a constitutional grandfather clause."[186] Despite its capabilities, at the end of the day the AIR program is largely made up of traditional surveillance techniques.[187] Though its digital integration may offer a hook for the Source Rule, that would mean that no modern aerial surveillance at all would be allowed, which seems unlikely.[188]

David Gray and Danielle Citron offer a similar solution. It stems from what they refer to as the "Fourth Amendment interest in quantitative privacy."[189] Much like Kerr's Source Rule, Gray and Citron avoid the mosaic theory messiness of "*how much* information is gathered in a particular case" by instead

---

[181] Orin Kerr (@OrinKerr), TWITTER (June 24, 2021, 2:08 PM), https://twitter.com/OrinKerr/status/1408124995373514765.

[182] *See* DANIEL SOLOVE & PAUL SCHWARTZ, PRIVACY LAW FUNDAMENTALS 38 (5th ed. 2019) (describing the differences between third party doctrine and plain view doctrine).

[183] *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't., 456 F. Supp. 3d 699, 719 (D. Md. 2020).

[184] Kerr, *Implementing Carpenter*, *supra* note 40, at 28.

[185] *Id.* at 40.

[186] *Id.* at 16.

[187] *Cf.* Florida v. Riley, 488 U.S. 445, 453 (1989) (recognizing that aerial surveillance techniques are becoming more commonly used as traditional surveillance techniques).

[188] *See id.*

[189] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 83 (2013).

"focus[ing] on *how* information is gathered."[190] They believe whether conduct constitutes a search depends on whether the technology used is capable of facilitating "broad and indiscriminate surveillance" that would intrude "upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents."[191] If the technology has this capacity, then using it is a search.[192] This definition more easily provides Fourth Amendment protection against the AIR program than Kerr's Source Rule, but there is still the issue of figuring out what government conduct would be a search when it comes to something like the AIR program.[193] Is all aerial surveillance a search? Or just the AIR program? If it is just the AIR program, where is the line at which some kind of aerial surveillance becomes a search? It seems like asking courts to resolve those questions would result in many of the same problems as the mosaic theory.

What's more, the *en banc* concurrences demonstrate that courts may not be in the best position to address the sweeping policy concerns dragnet surveillance implicates.[194] Under the mosaic theory, the Source Rule, or a quantitative privacy framework, judges must draw lines that are heavily influenced by policy concerns and compelling, but competing, interests.[195] As Justice Gorsuch pointed out in *Carpenter*, "Deciding what privacy interests should be recognized often calls for a pure policy choice, many times between incommensurable goods—between the value of privacy in a particular setting and society's interest in combating crime."[196] That is not to say that judges should never

---

190 Gray & Citron, *supra* note 189, at 71.

191 *Id.* at 72.

192 *Id.*

193 *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 23 (2008).

194 *See generally* Amnesty Int'l USA v. Clapper, 667 F.3d 163, 171 (2d Cir. 2011) (citing ACLY v. NSA, 493 F.3d 644, 650 (6th Cir. 2007)).

195 *See* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1823–24 (stating that "[t]o date, the Supreme Court has not adopted a single test for this assessment. Professor Orin Kerr has attempted to provide a comprehensive account of the various tests . . . the Court has used over time in defining reasonable expectation of privacy").

196 Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting).

make policy judgments—they can and do—but many of the key questions in this area are those of policy, not law. This counsels us to hesitate before trying to apply the Fourth Amendment to dragnet government surveillance like the AIR program.

Given the issues presented by this case in trying to apply Fourth Amendment protection to the AIR program, regardless of whether those issues occur because the Fourth Amendment should not apply doctrinally or because it cannot be applied practically, the Fourth Amendment is not a good answer to dragnet government surveillance. Fortunately, though, courts and the Fourth Amendment are not the only sources of protection for those concerned.

PART III:

So far, this Note has set up a conundrum: there is a problem, but the judiciary—the institution currently offering the predominant solution—should not offer a solution. In Part I, this Note discussed modern government surveillance techniques and the significant associated concerns that desperately need to be addressed. Part I also overviewed how courts have traditionally responded to some of those concerns. But Part II used *Leaders of a Beautiful Struggle* to argue that, despite the concerns and the historic role of courts, courts should not respond to the concerns created by dragnet government surveillance like the AIR program. The leading judicial solution, the mosaic theory, is difficult to apply and has a host of issues.[197] None of the Fourth Amendment alternatives seem like they would fare significantly better when dealing with something like the AIR program. This Part finally addresses that conundrum by arguing that the legislature can best deal with modern dragnet government surveillance.

This Part will briefly discuss why judicial action in this area could actively undermine efforts to address the concerns posed programs like the AIR program. Then, it will explain why the legislature is well-situated to address those concerns. Finally, it will explore possible legislative solutions and approaches.

---

[197] *See generally* Kerr, *supra* note 40; Fairbanks, *supra* note 77 (discussing further issues with the mosaic theory in addition to the problems specifically discussed with respect to *Leaders of a Beautiful Struggle*).

A. Dangers of Relying on Judicial Action

It is arguable that, while the courts alone may not offer a sufficient solution, until the legislature acts, the courts are better than nothing. After all, in *Leaders of a Beautiful Struggle*, the Sixth Circuit ultimately came down on the side of protecting privacy.[198] But this argument is wrong for two reasons. First, the mosaic theory does not reliably protect privacy.[199] Second, judicial action in this area could create legislative inaction.[200]

Leaders of a Beautiful Struggle does a good job of demonstrating why the mosaic theory does not offer reliable privacy protection.[201] Due to the difficulty of applying the mosaic theory, it is almost always easy for courts to justify upholding surveillance.[202] Both the district court and the Fourth Circuit panel found that the AIR program did not violate the Fourth Amendment. This relates to the general idea that the mosaic theory is not necessarily more privacy protective than traditional Fourth Amendment analysis.[203] As with the panel opinion, courts can rule that while some amount of surveillance would cross the line, the amount at issue does not run afoul of the Fourth Amendment. *Leaders of a Beautiful Struggle* could well have ended with either the district court or panel opinion, giving the AIR program a stamp of judicial approval and an air of legitimacy it may not deserve.

Even if courts could offer adequate privacy protection, it is unlikely that they could address all the surveillance issues necessary for courts' protection to be meaningful. It takes a long time for cases to work through the judicial process and the Supreme Court hears only a small number of Fourth Amendment cases each year.[204] As Ric Simmons has recognized, "Given the wide diversity of surveillance methods, the rapid advance of technology (which is both giving the government new

---

198 Leaders of a Beautiful Struggle v. Balt. Police Dep't., 2 F.4th 330, 342–43 (4th Cir. 2021).

199 *See id.*

200 Charles Weisselberg, *Mourning Miranda*, 96 CALIF. L. REV. 1519, 1579 (2208).

201 *See Leaders of a Beautiful Struggle*, 2 F.4th at 342–43.

202 *See* Fairbanks, *supra* note 77 (describing the issues mosaic theory faces); *see also* Wilson, Jr., *supra* note 155 (detailing additional issues within mosaic theory).

203 Fairbanks, *supra* note 77.

204 RIC SIMMONS, SMART SURVEILLANCE: HOW TO INTERPRET THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 26 (2019).

surveillance tools and creating new types of devices that the government needs to search), and our own constantly evolving expectations of privacy, there is no way the Court can provide enough guidance to police or to lower courts at that deliberative pace."[205]

Despite the fact that courts do not reliably offer protection from dragnet government surveillance, legislatures may not recognize this. Instead, they may mistakenly view courts' actions as sufficient and therefore choose not to address the issue themselves. As Charles Weisselberg explained in the *Miranda* context, when courts do "the work of policing the police," legislators have "little incentive" to act themselves.[206] Even worse, if legislatures are under the impression that courts use the Fourth Amendment to adequately protect against dragnet government surveillance, legislatures may believe that if they go too far, the courts will step in. Legislative inaction perpetuates the status quo.[207]

B. Reasons for Legislative Action

Unlike the courts, legislatures are well-positioned to address dragnet government surveillance. Somewhat ironically, this view has a long judicial pedigree, predating even *Katz*. In 1928, Chief Justice Taft wrote for the Court in *Olmstead v. United States* that the Fourth Amendment did not protect against wiretapping. He noted that "[t]he language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office" and that "[t]he intervening wires are not part of his house or office, any more than are the highways along which they are stretched."[208] Instead, Taft suggested that it was up to Congress to "protect the secrecy of telephone messages."[209] Roughly ninety years later, the

---

[205] SIMMONS, *supra* note 204.

[206] Weisselberg, *supra* note 189, at 1597.

[207] *See* Citron & Gray, *supra* note 9, at 389 ("The political branches have likewise left the expansion of surveillance technologies largely unchecked, save for a few reactionary pieces of legislation addressing a narrow range of concerns such as banking and telephone records").

[208] Olmstead v. United States, 277 U.S. 438, 465 (1928), *overruled in part by* Berger v. New York., 388 U.S. 41, 87 (1967), *and overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

[209] *Id.* Despite silence on the issue in *Katz*, Congress eventually did address wiretapping.

Carpenter dissents echoed Chief Justice Taft's view.[210] Justice Kennedy, in his dissent, recognized the difficulties of balancing new surveillance tools against new tools for committing crimes, stating:

> How those competing effects balance against each other, and how property norms and expectations of privacy form around new technology, often will be difficult to determine during periods of rapid technological change. In those instances, and where the governing legal standard is one of reasonableness, it is wise to defer to legislative judgments like the one embodied in § 2703(d) of the Stored Communications Act. In § 2703(d)[,] Congress weighed the privacy interests at stake and imposed a judicial check to prevent executive overreach. The Court should be wary of upsetting that legislative balance and erecting constitutional barriers that foreclose further legislative instructions. The last thing the Court should do is incorporate an arbitrary and outside limit—in this case six days' worth of cell-site records—and use it as the foundation for a new constitutional framework. The Court's decision runs roughshod over the mechanism Congress put in place to govern the acquisition of cell-site records and closes off further legislative debate on these issues.[211]

Justice Alito took a similar perspective, writing, "Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."[212] And Justice Gorsuch similarly pointed out that "[l]egislators are responsive to their constituents and have institutional resources designed to help them discern and enact majoritarian preferences."[213]

The justices are not alone in these views. Kerr argues that courts should "place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies."[214] Echoing Justice Gorsuch's view that legislators are more responsive to their constituents than are courts, Simmons agrees

---

[210] *See* notes 211-13 *infra* and accompanying text.

[211] Carpenter v. United States, 138 S. Ct. 2206, 2233 (2018) (Kennedy, J., dissenting) (internal citations omitted).

[212] *Id.* at 2261 (Alito, J., dissenting).

[213] *Id.* at 2265 (Gorsuch, J., dissenting).

[214] Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004).

by drawing on Slobogin's empirical work in the area and focusing on the difference between the Supreme Court's beliefs about privacy as compared to the general public.[215]

These views are particularly salient when discussing dragnet government surveillance like the AIR program. Slobogin refers to such surveillance programs as "panvasive surveillance." Panvasive surveillance is mass surveillance aimed at entire populations without any individual suspicion about the people being recorded.[216] Arguing that the political process offers a way for courts to navigate the issues surrounding dragnet government surveillance, Slobogin recognizes that "the political process is often well-situated to deal with panvasive searches and seizures because these searches and seizures affect wide swaths of the population that can have access to the legislature."[217]

Of course, a legislative solution is not a foregone conclusion. While this Note argues that the legislature is better equipped than courts to address the issues dragnet surveillance poses, that is by no means a guarantee that the legislature will take the necessary steps. As Sara Igo recognized in her exhaustive account of privacy in the United States, many lack faith that legislatures will pass the necessary laws to protect privacy.[218] One reason for this, Igo believes, is that "[t]he central state's own changing aspect—long in the making—from relatively beneficent bureaucracy to menacing invader."[219] But unlike courts, citizens have control over their legislatures and as privacy advocates continue their work, there will be more and more pressure on legislatures to act. And indeed, there have been movement and glimmers of hope in Congress suggesting that elected representatives are finally willing to truly address the threats posed by modern dragnet government surveillance.[220]

---

[215] *See* SIMMONS, *supra* note 204, at 27–28 (comparing the view of courts on privacy violations with the views of randomly sampled persons from the population, ultimately revealing a sharp difference in opinion on the issue).

[216] Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L. J. 1721, 1723 (2014).

[217] *See id.* at 1738. It should be noted Slobogin's article predated *Carpenter*, and Slobogin assumed that the Court would not apply the Fourth Amendment to most pervasive surveillance.

[218] *See* SARAH E. IGO, THE KNOWN CITIZEN 363 (2018) (discussing negative perception of state and regulatory agency actions to protect privacy concerns).

[219] *Id.*

[220] *See* Elizabeth Goetein, *Surprising Senate Vote Signals Hope for Surveillance Reform*, BRENNAN CNTR. FOR JUST. (May 16, 2020), https://brennancenter.org/our-work/analysis-opinion/surprising-senate-vote-

C. Possible Legislative Solutions

While it is easy to say that legislatures are better positioned than courts to address dragnet surveillance issues, it is far harder to identify how legislatures should act. Given the complexity of the topic and the rate of change, it would be impossible for this Note to provide a sufficient answer. Instead, this Note will examine some broader ideas that legislatures could employ in crafting solutions to dragnet government surveillance, using the surveillance from *Leaders of a Beautiful Struggle* as an example when necessary. This Note will also briefly discuss four specific proposals from privacy law scholars that provide clear frameworks for legislative action.

Unlike courts, legislatures are free to consider nearly anything when determining how to balance privacy concerns with legitimate needs for surveillance. As a starting point, legislatures, and even individual citizens, must consider broadly what it means to co-exist successfully with today's technologies. In *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*, Shannon Vallor explains the importance of actively cultivating a technomoral virtue ethic.[221] Vallor asks, "How can we begin to design and implement *now* educational and cultural projects to enhance the cultivation of technomoral virtue? For this is the only way to ensure that new surveillance technologies are deployed wisely to promote human flourishing in an increasingly opaque future."[222] Such a reframing of how technology and government surveillance are approached is likely necessary to sufficiently address the issues dragnet government surveillance poses.

Fortunately, privacy scholars have long been considering those ideas and developed more concrete suggestions. One noteworthy effort that the legislature could enact comes from Woodrow Hartzog's *Privacy's Blueprint: The Battle to Control the Design of New Technologies*.[223] Hartzog identifies a substantial list of

---

signals-new-hope-surveillance-reform (discussing strong bipartisan support for privacy concerns and signaling potential future steps); *see also* SHANNON VALLOR, TECHNOLOGY AND THE VIRTUES: A PHILOSOPHICAL GUIDE TO A FUTURE WORTH WANTING, 193–95 (2016) (arguing against "techno-fatalism").

[221] *See generally* VALLOR, *supra* note 220 (providing background on the topic of unrestricted AI research and offering a philosophical framework for its development).

[222] *Id.* at 207.

[223] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

surveillance technologies, which he terms "seeking technologies."[224] He then explains how to *design* those technologies to protect privacy: by "embracing data minimization" and "add[ing] friction."[225]

By "data minimization," Hartzog means that seeking technologies "should be designed to only collect and keep personal information that is directly relevant and necessary to accomplish a specified purpose. Once that purpose has been fulfilled, the data minimization principle dictates that the personal information is no longer necessary and should be deleted."[226] Some of this already exists in the AIR program used in *Leaders of a Beautiful Struggle*,[227] which placed limits on how long data could be stored and anonymized individuals (although their identities were easily revealed).[228] But stricter limits on data retention could have been built into the program in ways that were more closely aligned with the goals of the program. For example, if no violent crimes were reported in a given area within an hour, all images captured in that area for the past hour could have been immediately discarded.

By adding "friction," Hartzog means that transaction costs could be leveraged to "make information more or less accessible" depending on how "open or private" the legislatures want the programs to be.[229] It is hard to say exactly what this would look like in *Leaders of a Beautiful Struggle*, but integrating AIR data into other BPD surveillance systems would be a good starting point.

Notably, it would be difficult—if not impossible—for courts to be involved at the design stage of new surveillance techniques. Legislatures, however, are ultimately responsible for the funds that buy those technologies. Thus, they could enact specific design requirements aligned with Hartzog's suggestions at this early stage in the process.

To conclude, this Note briefly highlights several scholars' solutions to dragnet government surveillance that are more concrete than the ideas discussed above. The four highlighted—

---

[224] HARTZOG, *supra* note 223, at 245–50.
[225] *Id.* at 250–55.
[226] *Id.* at 251.
[227] Leaders of a Beautiful Struggle v. Balt. Police Dep't., F.4th 330, 334, 342 (4th Cir. 2021).
[228] *See id.*
[229] HARTZOG, *supra* note 223, at 253.

David Gray, Ric Simmons, Christopher Slobogin, and Daphna Renan—share similarities and include some of the broader concepts already reviewed.[230] Given that the scholars are better positioned to explain their ideas themselves, this Note does not do a deep analysis, but merely offers them examples of possibilities that legislatures can and should explore in this area.

Gray argues that legislatures can use the Wiretap Act as a model to follow when passing surveillance-curbing laws, and thus merely need to apply this model to new technologies.[231] Gray explains that requiring a court order before deploying certain surveillance technologies, as with the Wiretap Act, would be beneficial.[232] Although the Wiretap Act uses a probable cause standard that would not work for dragnet surveillance, legislatures could provide precise guidance to courts by legislating "a more fact-based test that weigh law enforcement and security interests against citizen privacy interests."[233] Combining this with the Wiretap Act's exhaustion requirement would add another layer of oversight to ensure surveillance programs were not being deployed unnecessarily.[234] This means that in *Leaders of a Beautiful Struggle*, the government would have had to convince a judge that there was (1) a need for the AIR program and (2) no good alternative to it. Similarly, and in alignment with Hartzog's views, Gray points out that "[m]inimization procedures like those required under the Wiretap Act would play a particularly important role in ensuring that [surveillance technology] deployments do not result to a de facto surveillance state."[235]

Simmons, alternatively, argues for legislative action based on a cost–benefit analysis. This analysis would serve as a transition to the eventual creation of an administrative agency responsible for regulating government surveillance.[236] In that world, courts would largely defer to the legislature or agency, and would rely on four guiding principles to navigate any remaining Fourth Amendment issues. These principles would be to (1) develop new binary surveillance tools, again echoing Hartzog; (2) encourage

---

[230] *See* discussion *supra* Part III.A.

[231] GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, *supra* note 13, at 254–60.

[232] *Id.* at 258–59.

[233] *Id.* at 259.

[234] *Id.*

[235] *Id.*

[236] SIMMONS, *supra* note 204, at 185–86.

low-cost surveillance methods; (3) enhance third-party rights; and (4) properly limit hyper-intrusive searches.[237]

Addressing what he calls "The Cloud," which is a system of databases under which the AIR program would definitely qualify, Slobogin provides four surveillance regulatory regimes for policymakers to enact.[238] Most relevant to dragnet government surveillance is the regime he classifies as "Event-Driven Cloud Access—Hassle Rates."[239] For something like gunshots that would trigger the AIR program response, "uses of The Cloud could result in a large haul of people, among whom may be the perpetrator or a witness, but many of whom will be neither."[240] Legislators should act to minimize "the 'hassle rate'—the proportion of innocent people subject to police investigation in an effort to find the one or two bad people."[241] Slobogin suggests that hassle rates "should probably vary with the type of information sought and the type of crime being investigated."[242] As with Gray and the Wiretap Act, Slobogin believes that law enforcement should be required to seek authorization from a judge before accessing Cloud data.[243]

Finally, Renan, addressing the difficulties of applying transactional (individualized) Fourth Amendment law to programmatic (dragnet) surveillance, argues for administrative governance of government surveillance.[244] While some of her analysis focuses on importing administrative law into Fourth Amendment law,[245] she also explores administrative law as an independent solution.[246] Referring specifically to surveillance programs that implicate the mosaic theory, Renan explains:

A framework statute like the APA could require this type of

---

[237] SIMMONS, *supra* note 204, at 186–89.

[238] Christopher Slobogin, *A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age*, NAT'L. CONST. CTR., https://constitutioncenter.org/digital-privacy/policing-and-the-cloud (last visited Feb. 2, 2023).

[239] *Id.* at 11.

[240] *Id.*

[241] *Id.* at 11–12.

[242] *Id.* at 12.

[243] *Id.*

[244] *See generally* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039 (2016) (discussing the tension between transactional Fourth Amendment law and programmatic surveillance which may be solved by the development of governance under an administrative law framework).

[245] *Id.* at 1077–88.

[246] *Id.* at 1091–127.

> program design to proceed under a rulemaking requirement, pursuant to principles of transparency, public input, and judicial review. An agency could be required to specify what types of information would be collected, how long the information would be retained, to what purposes it could be used, and with what agencies information could be shared. Administrative law also could require this type of surveillance rulemaking to address, for instance, whether and under what circumstances individuated searches in the license-plate-reader database require senior-level approval or a showing of individualized suspicion.[247]

These examples are not meant to be viewed as the only or best solutions legislatures could enact. Instead, these examples are meant to show that there are already tangible proposals out there, many of which share significant similarities. Ultimately—and this is one of the most significant advantages legislatures have over courts—this area will involve lots of experimentation. The sooner legislatures start that process, the better.

CONCLUSION

Modern dragnet government surveillance is all around us, presenting a myriad of serious issues that impact everyone. And there are no easy solutions to these issues. In an effort to do something, courts have fashioned a novel Fourth Amendment approach, the mosaic theory, to try to effectively analyze such surveillance.[248] Unfortunately, those efforts are misguided. *Leaders of a Beautiful Struggle* demonstrates both the type of surveillance that should concern everyone and the deficiencies of the mosaic theory in addressing that type of surveillance.[249] Though the mosaic theory sometimes leads to privacy protection where the traditional Fourth Amendment analysis may not, the mosaic theory's protection is unreliable because it is unclear how and when the mosaic theory should apply.[250] The mosaic theory further requires judges to make policy determinations they are not well-positioned to make, and it comes at a cost. *Leaders of a Beautiful Struggle* may have stopped one dragnet government surveillance program, but it leaves us to hope that courts are willing to stop the next one.[251] Moreover, so long as legislatures

---

[247] Renan, *supra* note 244, at 1051–53, 1092–93; *see also* discussion *supra* notes 39–76 and accompanying text.

[248] *See* discussion *supra* notes 39–76 and accompanying text.

[249] *See* discussion *supra* Part II.

[250] *See* discussion *supra* notes 39–76 and accompanying text.

[251] *See* discussion *supra* Part II.D.

think courts have a handle on government surveillance, they may fail to intervene when they otherwise would. Courts should therefore abandon the mosaic theory and leave specific types of surveillance that do not fit under the Fourth Amendment to legislatures. Then, legislatures can and should act to curb overly intrusive surveillance programs. Indeed, they must do so because "[p]rivacy is essential to be free and at ease," and "[w]e all need some time when nobody sees."[252]

The Eyemonger wiped tears from each of his eyes.
He had learned a hard lesson that made him quite wise.
Privacy is essential to be free and at ease.
We all need some time when nobody sees.[253]

[252] Solove, *supra* note 1.
[253] *Id.*