University of Maryland Francis King Carey School of Law

From the SelectedWorks of David C. Gray

2013

A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy

David C. Gray
Danielle Keats Citron, *University of Maryland Francis King Carey School of Law*

Available at: https://works.bepress.com/david_gray/21/

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 14, ISSUE 2: SPRING 2013

A SHATTERED LOOKING GLASS: THE PITFALLS AND POTENTIAL OF THE MOSAIC THEORY OF FOURTH AMENDMENT PRIVACY

***David Gray**[*] **& Danielle Keats Citron**[**]*

On January 23, 2012, the U.S. Supreme Court issued a landmark non-decision in United States v. Jones*. In that case, officers used a GPS-enabled device to track a suspect's public movements for four weeks, amassing a considerable amount of data in the process. Although ultimately resolved on narrow grounds, five Justices joined concurring opinions in* Jones *expressing sympathy for some version of the "mosaic theory" of Fourth Amendment privacy. This theory holds that we maintain reasonable expectations of privacy in certain quantities of information even if*

[*] Associate Professor, University of Maryland Francis King Carey School of Law.

[**] Lois K. Macht Research Professor of Law, University of Maryland Francis King Carey School of Law, Affiliate Scholar, Stanford Center on Internet and Society, Affiliate Fellow, Yale Information Society Project. The authors thank everyone who generously commented on this work during presentations at the Information Society Project at Yale Law School, the Annual Meeting of the ABA/AALS Criminal Law Section, the University of North Carolina, Northwestern University, and Yale's Conference on Locational Privacy and Biometrics, and during conversations at the Privacy Law Scholars Conference, the American Law Institute Meeting on Information Privacy Law, and the Harvard Law Review Symposium on Informational Privacy. Particular thanks go to Jack Balkin, Richard Boldt, Becky Bolin, Mary Bowman, Al Brophy, Andrew Chin, Bryan Choi, Thomas Clancy, Julie Cohen, LisaMarie Freitas, Susan Freiwald, Don Gifford, Mark Graber, James Grimmelmann, Deborah Hellman, Camilla Hrdy, Renée Hutchins, Orin Kerr, Joseph Kennedy, Catherine Kim, Anne Klinefelter, Michael Mannheimer, Dan Markel, Christina Mulligan, Richard Myers, Neil Richards, Catherinc Sabbeth, Laurent Sacharoff, Paul Schwartz, Christopher Slobogin, Robert Smith, Dan Solove, Max Stearns, David Super, Peter Swire, Peter Quint, Jason Weinstein, Arthur Weisburd, and Jonathan Witmer-Rich. Liz Clark Rinehart provided critical research assistance and Max Siegel insightful editorial work. The authors are also grateful to Frank Lancaster for holding us together.

we do not have such expectations in the constituent parts. This Article examines and explores the mosaic theory. This Article concludes that the mosaic theory exposes an important quantitative dimension of Fourth Amendment privacy but raises serious practical challenges, which, as argued elsewhere, can be met by regulating surveillance technologies capable of facilitating broad programs of indiscriminate surveillance.

I. INTRODUCTION

Since the first etchings of the ancients, integrity and authenticity have stood as pillars of ethics. Whether inspired by religious faith or deontological reflection, the very concepts of a good life and a life well-lived imply the pursuit of some measure of coherency, consistency, and self-possession. This search for order is distinguished from the otherwise fragmented moments, contexts, and pursuits that occupy our existences. From a phenomenological point of view, this amounts to a tautology. After all, the notion of the self is tied to persistence of identity through time and space.[1]

Beyond questions of description and definition, however, lie more compelling questions of freedom, liberty, dominance, and oppression. Although it is a necessary condition of liberty, persistence of identity through time is hardly sufficient to secure liberty. In fact, it is a point of vulnerability. What better marker of oppression could we imagine than using disciplinary structures to occupy and control experiences, places, and activities in order to shape and construct the identities and lives of subjects?

Some have argued that even a fully constructed self is "free" in the sense that conduct is neither coerced nor compelled against one's will.[2] But this account of freedom is far too thin to accommodate American conceptions of liberty. When we declare

---

[1] *See* JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING 226–27 (T. Tegg and Son, 27th ed. 1836) (1690).

[2] *See, e.g.*, ALFRED JULES AYER, *Freedom and Necessity*, *in* PHILOSOPHICAL ESSAYS 271 (1969).

the inalienable right to "life, liberty, and the pursuit of happiness,"[3] we mean more than mere freedom from external constraint. We herald both the right to define for ourselves what that good life entails and to pursue it free from unreasonable constraint. In this thicker, ethical sense, to be free is to pursue a lifelong process of self-understanding and self-development. A state committed to securing this brand of liberty for its citizens must therefore do more than merely protect individuals from situational coercion; it must secure the space needed to become and to be. In keeping with our commitments to this brand of liberty, we provide broad constitutional protections for freedom of speech, conscience, and religion.

Understood as the conditions necessary to our projects of ethical self-construction, freedom and liberty naturally entail privacy. Observation and surveillance are mainstays for programs of discipline and constraint. Jeremy Bentham's *Panopticon* provides the most ready trope,[4] but, as Michel Foucault has documented, surveillance, and the ambient possibility of surveillance, play central roles in a wide range of institutions—such as prisons, schools, and mental institutions—that are designed to constrain and construct their subjects.[5] In the proper context, and subject to appropriate controls, these tools of constitutive observation play an important and necessary social role. Plato's famous parable of the Ring of Gyges paints a vivid picture of the alternative, showing us the deleterious effects of absolute anonymity on behavior and character.[6] Because it leads to

---

[3] THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

[4] *See generally* JEREMY BENTHAM, PANOPTICON: OR THE INSPECTION HOUSE (1791) (stating that a Panopticon is a rotunda in which the observers are situated in the center and the observed occupy the outer area, allowing a small number of observers to watch over a large number of subjects).

[5] *See generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195–210 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977) (explaining how prisons use both surveillance and the threat of surveillance to modify prisoner conduct and consciousness).

[6] Plato, *Republic: Book II*, *in* FIVE GREAT DIALOGUES 253, 484 (Louise Ropes Loomis ed., B. Jowett trans., 1942). The parable is as follows:

conformity with rules and norms,[7] surveillance is, in this sense, a necessary condition of self and society, and therefore liberty as well. Thus, in the United Kingdom, which monitors various locations using a sizeable closed-circuit television program, the House of Lords found that the constant surveillance made people feel more "safe," even when the program showed "mixed results" in crime detection and prevention.[8] At the same time, surveillance can also be a tool of oppression. That is why programs of broad and indiscriminate surveillance are frequent hallmarks of tyrannical regimes, both real and fictitious.[9]

> Suppose now that there were two such magic rings [allowing the wearer to become invisible], and the just put on one of them and the unjust the other; no man can be imagined to be of such an iron nature that he would stand fast in justice. No man would keep his hands off what was not his own when he could safely take what he liked out of the market, or go into houses and lie with any one at his pleasure, or kill or release from prison whom he would, and in all respects be like a god among men . . . . And this we may truly affirm to be a great proof that a man is just, not willingly or because he thinks that justice is any good to him individually, but of necessity, for wherever anyone thinks that he can safely be unjust, there he is unjust . . . . If you could imagine any one obtaining this power of becoming invisible, and never doing any wrong or touching what was another's, he would be thought by the lookers-on to be a most wretched idiot, although they would praise him to one another's faces, and keep up appearances with one another from a fear that they too might suffer injustice.

Id. at 257–59.

[7] Even images of eyes can lead to more honest behavior, as researchers found in a study that showed more people cleaned up after themselves in a cafeteria when there was a poster of eyes instead of flowers. Sander van der Linden, *How the Illusion of Being Observed Can Make You a Better Person*, SCI. AM. (May 3, 2011), http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person.

[8] CONSTITUTIONAL Committee, SURVEILLANCE: CITIZENS AND THE STATE, 2008–9, H.L. 18-I, ¶¶ 70–78 (U.K.), *available at* http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf.

[9] *See* ORLANDO FIGES, THE WHISPERERS: PRIVATE LIFE IN STALIN'S RUSSIA 258–59 (Picador reprint 2008) (2007) (describing a system of "mutual surveillance" in which people were expected to spy on their families, coworkers and neighbors, including those living with them in communal apartments); GEORGE ORWELL, 1984 (Rosetta Books ed. 2000) (1949) (painting a vivid picture of life under a regime that exercises constant surveillance as a tool of

For these reasons, surveillance presents a bit of a conundrum for social and political theory because it is at once a condition of a free self and a potential threat against liberty. A central preoccupation of information privacy law scholars has been to chart the boundaries between observational and surveillance practices that are liberty enhancing and those that are liberty denying. At least since Samuel Warren and Louis Brandeis's canonical 1890 article, technology has been a key player.[10]

Despite that thread of connection to the past, there can be no doubt that we live in very different times than Warren and Brandeis and confront more dramatic consequences for privacy as a result of modern technologies.[11] Whereas Warren and Brandeis feared the impact of film cameras taking still images on privacy,[12] we live in a world populated by closed-circuit television networks, high-resolution spy satellites, surveillance drones, and Global

---

social control); Julian Ryall, *North Korea Steps Up Surveillance of Citizens with 16,000 CCTV Cameras*, TELEGRAPH (Jan. 15, 2013), http://www.telegraph.co.uk/news/worldnews/asia/northkorea/9801850/North-Korea-steps-up-surveillance-of-citizens-with-16000-CCTV-cameras.html (reporting that North Korea now has over 101,000 cameras with which to "tighten[] its control on the lives of the people").

[10] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (explaining that recent inventions call attention to the next step to be taken for the protection of the person and the right to be let alone).

[11] *See* Christopher Slobogin, *An Original Take on Originalism*, 125 HARV. L. REV. F. 14, 19 (2011) (explaining "that in many areas relevant to search and seizure we do not have a good historical account" and that many cases "do not have analogues, even tenuous ones," such as "special needs cases, involving a wide range of regulatory intrusions such as drug testing and searches of students and employees, roadblocks set up to detect illegal immigrants, and anti-terrorist checkpoints at airports, subways, ferries, and dams" which "raise the most contentious and important Fourth Amendment issues courts are addressing today").

[12] *See* Warren & Brandeis, *supra* note 10, at 195 ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' ").

Positioning System ("GPS") tracking technology.[13] In the late nineteenth century, what personal information was collected appeared in the paper files of isolated agencies and corporations.[14] At the beginning of the twenty-first century, agencies and corporations can access nearly infinite storage capacity, integrated data systems, powerful data aggregation technologies, and increasingly sophisticated data mining tools.[15] With this dramatically enhanced capacity to aggregate, store, and share information comes corresponding threats to privacy.

In themselves, and in the aggregate, technological advances have made it possible for public and private actors to watch us and to know us in ways that once seemed like science fiction. Take, for example, the "Virtual Alabama" project, a collaboration between Alabama and Google.[16] Virtual Alabama is a data

---

[13] *See* Brandon C. Welsh & David P. Farrington, *Public Area CCTV and Crime Prevention: An Updated Systemic Review and Meta-Analysis*, 26 JUST. Q. 716, 717 (2009); Siobhan Gorman, *Satellite-Surveillance Program To Begin Despite Privacy Concerns*, WALL ST. J. (Oct. 1, 2008), http://online.wsj.com/article/SB122282336428992785.html?mod=googlenews_wsj; Ryan J. Reilly, *FBI GPS Tracking Memos Kept Mostly Secret by Justice Department*, HUFFINGTON POST (Jan. 16, 2013), http://www.huffingtonpost.com/2013/01/16/fbi-gps-tracking-memos_n_2488180.html; Andrea Stone, *Drone Program Aims To 'Accelerate' Use of Unmanned Aircraft by Police*, HUFFINGTON POST (May 22, 2012), http://www.huffingtonpost.com/2012/05/22/drones-dhs-program-unmanned-aircraft-police_n_1537074.html.

[14] *See* ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 357 (James Waldo et al. eds., 2007) (explaining that the majority of record-keeping in the late 19th century was local and therefore limited in its ability to control individuals); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 246 n.11 (2006) (citing ELTING E. MORISON, MEN, MACHINES, AND MODERN TIME 54 (1966)); *see, e.g.*, *Early Census Processing and the Seaton Device*, U.S. CENSUS BUREAU, http://www.census.gov/history/www/innovations/technology/early_census_processing_and_the_seaton_device.html (last visited Apr. 4, 2013) (describing the laborious and time-consuming process of hand-processing census information).

[15] *See* Citron, *supra* note 14, at 247 (chronicling the rapid evolution of data collection and data processing).

[16] *See* Corey McKenna, *Virtual Alabama Facilitates Data Sharing Among State and Federal Agencies*, DIGITAL COMMUNITIES (Aug. 13, 2009),

aggregation system that combines three-dimensional satellite and aerial imagery, geospatial analytics, feeds from traffic cameras, private and public video systems (including feeds from one thousand five hundred schools), GPS location data, sex offender registries, hospital inventories, and land-ownership records, including assessments.[17] At present, the ever-expanding scope and reach of this technology is unchecked by constitution or statute, suggesting that Big Brother[18] is closer than we might think.

Governments are not the only ones using modern surveillance and data aggregation technologies to track and monitor our activities. Vast reservoirs of our private data are gathered by or otherwise reside in the hands of private entities.[19] GPS chips in our telephones, cars, and computers share a steady stream of locational information with companies providing services associated with these devices.[20] Internet Service Providers ("ISPs") log our online movements using "Deep-Packet Inspection."[21] Credit card companies and behavioral advertisers record and analyze our shopping habits, online and offline.[22] In one apocryphal case revealed in 2012, Target used information drawn from its internal

---

http://www.digitalcommunities.com/articles/Virtual-Alabama-Facilitates-Data-Sharing-Among.html.

[17] *See id.*

[18] *See* ORWELL, *supra* note 9.

[19] *See* Citron, *supra* note 14, at 248; Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 24–25 (2012) (responding to Professor Kerr's criticism of the difficult questions raised by mosaic theory).

[20] *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 679 (2011).

[21] *See* Danielle Keats Citron, *The Privacy Implications of Deep Packet Inspection*, *in* OFFICE OF PRIVACY COMM'R OF CAN., DEEP PACKET INSPECTION ESSAY PROJECT (2009), *available at* http://www.priv.gc.ca/information/research-recherche/2009/keats-citron_200903_e.asp

[22] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG., Feb. 16, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shoppinghabits.html?pagewanted=all&_r=0 (recounting how Target uses publicly available databases and market analytics to identify women who are in the early stages of pregnancy).

and exogenous databases to identify newly pregnant women who, they believed, would be particularly amenable to direct marketing of products for new mothers and their infants.[23] Target and other retailers also use ever more sophisticated behavioral and even neurological analytics in order to drive sales.[24]

As these new surveillance technologies have migrated from science fiction to reality over the last several decades, privacy scholars have updated and expanded upon Warren and Brandeis's warnings.[25] Principal among their concerns are the effects of continuous, indiscriminate, and often invasive surveillance on our abilities to pursue and enjoy basic liberties.[26] Privacy scholars have documented the risks and realities of abuse by those who acquire and hold substantial quantities of personal data.[27] As our lives have become increasingly dependent on data reservoirs, they

---

[23] *Id.*

[24] *Id.*

[25] *See, e.g.*, Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1831–32 (2010) (proposing "potential strategies for ensuring privacy tort law's efficacy in the information age" that build upon the theories of Warren and Brandeis); Diane L. Zimmerman, *Requiem for A Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 362–63 (1983) (arguing that, as technological intrusions become more prevalent, privacy law should focus on the source of the information, rather than whether it is exposed to the public).

[26] *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE 141 (2012); Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 195 (2008); Freiwald, *supra* note 20, at 679; Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 837 (2000); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 905, 931–39 (2009); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); Paul M. Schwartz, *Privacy and Participation: Personal Information and the Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560–61 (1995).

[27] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 44–47 (2004); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 33 (2008); Danielle Keats Citron, *Fulfilling Government's 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822 (2010); Citron, *supra* note 25, at 1805; Citron, *supra* note 14.

have warned us about the dangers of error and misinformation.[28] Despite these calls for concern, however, courts mostly have stayed out of the fray.[29] 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.[30]

All of this seems about to change. On January 23, 2012, in *United States v. Jones*,[31] the U.S. Supreme Court had the opportunity 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

---

[28] *See* Citron, *supra* note 25.

[29] *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1025 (2010) (describing case law on Internet communication, surveillance and data breaches as "sparse"). *But see* U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989) (prohibiting the disclosure of FBI rap sheets to third parties under FOIA); Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971) (limiting the dissemination of arrest records).

[30] *See, e.g.*, SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745 (1984) ("In 1978, in response to this Court's decision in United States v. Miller, . . . Congress enacted the Right to Financial Privacy Act . . . . That statute accords customers of banks and similar financial institutions certain rights to be notified of and to challenge in court administrative subpoenas of financial records in the possession of the banks."); M. Todd Heflin, *Who's Afraid of the Big Bad Wolf: Why the Fear of Carnivore Is an Irrational Product of the Digital Age*, 107 DICK. L. REV. 343, 352 (2002) ("Partially in response to the Court's decision in *Katz*, Congress codified Fourth Amendment principles, as applied to oral and written communications, in Title III of the Omnibus Crime and Safe Streets Act of 1968 . . . ."); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 857–58 (2002) (describing the controversial confirmation hearings of Judge Robert Bork's Supreme Court nomination leading up to Congress's passage of the Video Privacy Protection Act of 1988); Robert Ditzion, Note, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1322–23 n.5 (2004) (explaining that the Supreme Court's holding in *Smith v. Maryland*—that the use of pen registers to record telephone numbers did not implicate the Fourth Amendment—led to Congress passing limited regulations on government use of the technology and citing to the Electronic Communications Privacy Act of 1986).

[31] 132 S. Ct. 945 (2012).

proxies. Although the Court demurred for the time being, a majority of the sitting Justices expressed sympathy for what has come to be known as the "mosaic theory" of Fourth Amendment privacy.[32] 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 reasonable expectations of privacy in the constituent parts of that whole.[33]

This Article examines and explores the mosaic theory. Although the debate is in its early stages, the mosaic theory exposes an important, but heretofore underappreciated, quantitative dimension of Fourth Amendment privacy.[34] Nevertheless, the proposals made so far to convert that insight into a set of workable rules and principles are unconvincing. Part II provides a detailed exegesis of the mosaic theory by reviewing *Jones* and its predecessor litigation in the U.S. Court of Appeals for the District of Columbia Circuit. Part III reviews and expands upon the major conceptual, doctrinal, and practical objections that have been raised in the literature. Part IV deepens the discussion by exploring responses that mosaic advocates might make in defense of their theory. Part V concludes that, for the mosaic theory to be a serious response to the disconcerting encroachment of modern surveillance technologies on our reasonable expectations of privacy, its proponents must develop a practical means of implementation. Although it is beyond the scope of this Article,

---

[32] *See* Slobogin, *supra* note 19, at 3–4; *see also* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012).

[33] *See* Ryan Calo, *Don't Let Privacy Go To The Dogs: A Proposal To Wait On Jardines*, USVJONES.COM (June 2, 2012), http://usvjones.com/2012/06/02/dont-let-privacy-go-to-the-dogs-a-proposal-to-wait-on-jardines/ (implying that the mosaic theory does not address the use of drones for dragnet surveillance); Woodrow Hartzog, United States v. Jones *and the Need to Embrace Obscurity*, USVJONES.COM (June 2, 2012), http://usvjones.com/2012/06/02/united-states-v-jones-and-the-need-to-embrace-obscurity/ (concluding that the mosaic theory supports an obscurity-based analysis of privacy).

[34] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

the authors argue elsewhere that any such proposal must focus on the technologies.[35]

II. THE MOSAIC THEORY OF FOURTH AMENDMENT PRIVACY

Although privacy scholars have been beating a steady drum against the threats of broad and indiscriminate surveillance posed by contemporary advancements in surveillance technology, there has been relatively little resistance from legislatures and courts.[36] To be sure, there are some exceptions. Public discomfort with the unprecedented data mining and data sharing "Total Information Awareness" system under development at the Department of Defense in the late 1990s and early 2000s[37] resulted in Congress's cutting funding in 2004.[38] But that system has resurfaced in other governmental surveillance programs, just with different names, like "fusion centers."[39] Congress recently expressed concerns about fusion centers, which are cooperative data gathering, aggregation, and analysis ventures among local, state, and federal agencies in collaboration with private-sector allies,[40] but has yet to suggest any serious plans to regulate the use of these or any other

---

[35] *See* David Gray & Danielle Keats Citron, *Quantitative Privacy*, 98 MINN. L. REV. (forthcoming 2013).

[36] *See supra* notes 28–30 and accompanying text.

[37] *See* John Markoff, *Chief Takes Over at Agency To Thwart Attacks on U.S.*, N.Y. TIMES (Feb. 13, 2002), http://www.nytimes.com/2002/02/13/us/chief-takes-over-at-agency-thwart-attacks-on-us.html; Jeffrey Rosen, *Total Information Awareness*, N.Y. TIMES (Dec. 15, 2002), http://www.nytimes.com/2002/12/15/magazine/15TOTA.html; William Safire, *You Are a Suspect*, N.Y. TIMES (Nov. 14, 2002), http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html.

[38] Department of Defense Appropriations Act of 2004, Pub. L. No. 108-87, § 8131, 117 Stat. 1054, 1102 (2003).

[39] *See* U.S. SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 1 (2012), *available at* http://www.fas.org/irp/congress/2012_rpt/fusion.pdf.

[40] *See id.* ("The Subcommittee investigation found that DHS-assigned detailees to the fusion centers forwarded 'intelligence' of uneven quality—often times shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism.").

surveillance technologies.[41] In the face of persistent inaction by the legislature, courts have begun to step into the breach.[42] In this transformative environment, the Supreme Court granted certiorari in *United States v. Jones*.[43]

In 2004, a joint task force of federal and local law enforcement in Washington, D.C. began investigating a narcotics conspiracy that included Lawrence Maynard and Antoine Jones.[44] During the course of their investigation, officers sought and received warrants that allowed them to tap Maynard's and Jones's phones and to attach and monitor a GPS-enabled tracking device[45] to Jones's automobile.[46] The GPS warrant required that the officers install

---

[41] Both Democrat- and Republican-sponsored bills attempting to regulate surveillance died in committee last session. *See, e.g.*, Preserving Freedom from Unwarranted Surveillance Act of 2012, S. 3287, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/s3287/text; Protecting America's Privacy Act of 2012, S. 3515, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/s3515/text (limiting the overseas acquisition of information about a persons believed to be in the United States). *But see* Natasha Singer, *Their Apps Track You. Will Congress Track Them?*, N.Y. TIMES (Jan. 5, 2013), http://www.nytimes.com/2013/01/06/technology/legislation-would-regulate-tracking-of-cellphone-users.html?_r=0 (reporting on Senator Al Franken's continued effort to regulate the use of tracking technology in cell phones); *cf.* Location Privacy Protection Act of 2012, S. 1223, 112th Cong. (2012), *available at* http://www.judiciary.senate.gov/legislation/upload/HEN12877-Franken-Sub.pdf. (proposing controls on government and private access to locational data acquired through cellular phones and GPS devices).

[42] *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

[43] United States v. Jones, 132 S. Ct. 945 (2012)

[44] *Id.* at 948 (majority opinion); United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945.

[45] *See* Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 411–13 (2007) (explaining GPS-enabled tracking technology).

[46] *Jones*, 132 S. Ct. at 948. The vehicle in question was registered to Jones's wife, but the Government conceded, and the district court found, that Jones had a reasonable expectation of privacy in the Jeep. *Maynard*, 615 F.3d at 555–56 n.*. The Supreme Court later held that Jones also had a property interest in the Jeep. *Jones* 132 S. Ct. at 948. All courts therefore referred to the Jeep as "Jones's."

the device within ten days and within the District of Columbia.[47] Unfortunately, officers violated both of these terms, installing the device a day late and while Jones's vehicle was parked in a suburban Maryland parking lot.[48] They nevertheless used the device to track Jones for twenty-eight days, during which time they collected over two thousand pages of tracking data.[49]

Based on the officers' failure to abide the terms of their warrant, Jones moved at trial to suppress all evidence discovered by or through the GPS device.[50] The trial court, relying on *United States v. Knotts*,[51] denied his motion.[52] In *Knotts*, the United States Supreme Court held that using a radio beeper device to track a defendant over the course of an afternoon did not violate the subject's reasonable expectations of privacy because he had knowingly exposed himself to public observation.[53] Therefore, the beeper tracking was "neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment."[54] The trial judge in Jones's case saw no distinction between surveillance conducted using GPS and surveillance conducted using a beeper device because, in both cases, the technology revealed nothing more to officers than what the subjects had knowingly exposed to the public: their movements along public roads.[55] Although the officers in *Jones* violated the terms of their warrant, the trial court found that they were not required to get a warrant in the first place, and therefore did not violate Jones's Fourth Amendment rights.[56]

Based in part on evidence produced using the GPS-enabled tracking device, Jones was convicted.[57] On appeal, the United States Court of Appeals for the District of Columbia Circuit

---

[47] *Jones*, 132 S. Ct. at 948.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] United States v. Knotts, 460 U.S. 276, 281 (1983).
[52] *Jones*, 132 S. Ct. at 948.
[53] *Knotts*, 460 U.S. at 282–85.
[54] *Id.* at 285.
[55] *Jones*, 132 S. Ct. at 948.
[56] *Id.*
[57] *Id.* at 949.

reversed.[58] Writing for a unanimous panel, Judge Ginsburg held that *Knotts* did not control.[59] *Knotts*, he wrote, "held only that 'a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,' not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end."[60] Furthermore, he argued, there is a constitutionally significant difference between being tracked and monitored for an afternoon and being tracked and monitored twenty-four hours a day for four weeks.[61] The constitutional line, according to Judge Ginsburg's opinion, is marked by reasonable expectations of privacy.[62]

We knowingly expose ourselves to public observation whenever we leave the house. We must therefore expect that we will sometimes be observed during the course of our daily lives. According to Judge Ginsburg, however, the same cannot be said of our public movements in the aggregate.[63] Quite to the contrary, we reasonably expect that we are not being watched constantly.[64] Thus, according to Judge Ginsburg's panel, constant and sustained government surveillance constitutes a "search" for Fourth

---

[58] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945.

[59] *Id.* at 556.

[60] *Id.* at 557.

[61] *Id.* at 556–57.

[62] *Id.* at 557.

[63] *Id.* at 558; *see also id.* at 563 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects, each of those movements to remain 'disconnected and anonymous.' ").

[64] In an analogous way, state harassment laws and privacy tort law have reinforced the notion that people can expect to be free from unreasonable surveillance. *See, e.g.*, Galella v. Onassis, 487 F.2d 986, 998–99 (2d Cir. 1973) (upholding an injunction against a persistent paparazzo); Wolfson v. Lewis, 924 F. Supp. 1413, 1433–34 (E.D. Pa. 1996) (enjoining surveillance of a family on the grounds it was part of "a persistent course of hounding, harassment and unreasonable surveillance, even if conducted in a public or semi-public place").

Amendment purposes.[65] Because Jones had a "reasonable expectation of privacy in his movements over the course of a month . . . , and the use of the GPS device to monitor those movements defeated that reasonable expectation,"[66] the officers in *Jones* were obliged to submit themselves to Fourth Amendment constraints.[67] By violating the terms of their warrant, they failed in that duty.[68] The circuit court therefore vacated Jones's conviction.[69]

On certiorari, the United States Supreme Court affirmed.[70] Writing for the majority, Justice Scalia held that the officers' installation of the GPS device was a search because it was accomplished by a trespass and for the purpose of obtaining information.[71] According to Justice Scalia, "We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[72] Because the officers violated the terms of their warrant when installing the device, they violated Jones's Fourth Amendment rights.[73] All subsequent monitoring of the device was

---

[65] *Maynard*, 615 F.3d at 567 (citing Delaware v. Prouse, 440 U.S. 648, 662–63 (1979)).

[66] *Id.* at 563.

[67] *See id*. at 566–68.

[68] *Id.*

[69] According to its decretal paragraph, the court "reversed" Jones's conviction, but one assumes that the court intended to leave open the possibility of a retrial if the Government chose to go forward without evidence obtained by the GPS-enabled monitoring. *See, e.g.*, *id.* at 568 ("To be sure, absent the GPS data a jury reasonably might have inferred Jones was involved in the conspiracy.").

[70] United States v. Jones, 132 S. Ct. 945, 954 (2012).

[71] *Id.*; *see also* United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) ("[W]hen the government *does* engage in a physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.").

[72] *Jones*, 132 S. Ct. at 949.

[73] *See id.* at 949, 954 (citing *Maynard*, 615 F.3d 544) (affirming the decision of the Court of Appeals for the D.C. Circuit that "reversed the conviction because of admission of the evidence obtained by warrantless use of the GPS device which, it said, violated the Fourth Amendment"). Judge Kavanaugh proposed trespass as a narrower ground for the decision in his dissent from the

a fruit of this initial violation, so Justice Scalia saw no need to address the broader question of whether using the device to track Jones might constitute a separate and independent Fourth Amendment search.[74]

Writing for himself and three other Justices, Justice Alito concurred.[75] After expressing considerable skepticism about the majority's trespass rule, Justice Alito focused his attention on defending the basic premises of the quantitative theory of Fourth Amendment privacy upon which Judge Ginsburg relied in the court below.[76] For Justice Alito, the central Fourth Amendment issues presented to the Court by the facts in *Jones* arose from the use of new surveillance technologies. "In the pre-computer age," he wrote, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[77] It was simply impossible for law enforcement to conduct continuous surveillance of a suspect for four weeks using only traditional techniques.[78] As a consequence of these practical limitations, Justice Alito echoed the circuit court's point that we have good reason to believe that we are not subject to constant surveillance.[79] Although "short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," Justice Alito wrote, "longer term GPS monitoring in investigations of most offenses impinges on expectations of

---

circuit court's denial of the petition for rehearing en banc. *See* United States v. Jones, 625 F.3d 766, 769–71 (D.C. Cir. 2010) (Kavanaugh, J., dissenting).

[74] *See Jones*, 132 S. Ct. at 954.

[75] *Id.* at 957 (Alito, J., concurring).

[76] *Id.*

[77] *Jones*, 132 S. Ct. at 963.

[78] *Id*.

[79] *Id.* at 963–64; United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012) ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there . . . ."); *see also* Hutchins, *supra* note 45, 455–56.

privacy." [80] Despite joining the majority opinion, Justice Sotomayor wrote a separate concurrence in *Jones* to express broad sympathy with Justice Alito's quantitative approach to assessing Fourth Amendment privacy interests.[81]

The general theory of Fourth Amendment privacy advanced by Justice Alito, Justice Sotomayor, and Judge Ginsburg in these opinions has been described as the mosaic theory.[82] Although its various proponents differ in the details, the core insight that drives the mosaic theory of Fourth Amendment privacy is that we can maintain reasonable expectations of privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of those wholes.[83] Although it was not adopted in *Jones*, there appear to be five votes on the Court for adopting some version of the mosaic theory.[84] As a consequence, in the months after *Jones* there has been a rush of commentary on the conceptual, doctrinal, and practical viability of the mosaic theory.[85] The remainder of this Article will review and add to this

---

[80] *Jones*, 132 S. Ct. at 963–64 (2012) (Alito, J., concurring); *see also* Stephen Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 547–48 (2005) (describing the direct relationship between privacy expectations and factors such as duration of travel and route complexity).

[81] *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring).

[82] *See Maynard*, 615 F.3d at 562; Kerr, *supra* note 32, at 311. Justice Alito does not adopt the phrase "mosaic theory," but neither does he indicate any point of disagreement with Judge Ginsburg's basic mosaic framework. *See Jones*, 132 S. Ct. at 963–64. The term "mosaic" is borrowed from national security law, where the Government has defended against requests made under the Freedom of Information Act on the grounds that when otherwise innocuous information is aggregated it can reveal secret methods and sources. *See generally* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

[83] *See* Daniel Solove, United States v. Jones *and the Future of Privacy Law: The Potential Far-Reaching Implications of the GPS Surveillance Case*, USVJONES.COM (June 1, 2012), http://usvjones.com/2012/06/01/the-potential-far-reaching-implications-of-the-gps-surveillance-case/#more-146 (approving of the mosaic theory's expansion of privacy).

[84] *See Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring); *id*. at 957 (Alito, J., concurring in an opinion joined by Justices Ginsburg, Breyer, and Kagan).

[85] *See infra* Parts III & IV.

debate, beginning with an overview of the main challenges brought by critics and skeptics of the mosaic theory.

III. THE MOSAIC THEORY AND ITS DISCONTENTS

In the months after *Maynard* and *Jones*, the mosaic theory has been subject to considerable criticism both inside and outside the courts. Most of these objections fall into one of three categories: conceptual, doctrinal, and practical. This Part describes the most prominent and compelling objections in each of these categories and contributes a few more along the way. The conversation in subsequent Parts considers some responses that have been advanced by defenders of the mosaic theory, proposes a few more, and concludes that the mosaic theory cannot be dismissed prematurely, but that proponents bear the considerable burden of addressing practical concerns.

A. *Conceptual Objections to the Mosaic Theory*

Critics have met the mosaic theory with a basic arithmetical challenge that inheres in the mosaic approach itself. The mosaic theory is not needed to protect information that is already secured behind the veil of reasonable expectations of privacy. The mosaic theory is needed, and is therefore salient, only when the conduct or information at issue does not, when considered discretely, implicate reasonable expectations of privacy. The mosaic theory holds that, in some cases, certain quanta of data, or perhaps certain quanta of certain kinds of data,[86] implicate reasonable expectations of privacy even though the constituent parts do not.[87] So framed,

---

[86] *See Jones*, 132 S. Ct. at 954 (criticizing Justice Alito's suggestion that seriousness of the target crime might be a factor in assessing the Fourth Amendment analysis of informational mosaics). As we argue elsewhere, there are good doctrinal grounds for courts to include the seriousness of suspected criminal conduct when conducting the balancing of interests that Fourth Amendment reasonableness demands. *See infra* notes 75–83 and accompanying text.

[87] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *Maynard*, 615 F.3d at 558. The *Maynard* opinion recounts several compelling examples:

> 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

the mosaic theory seems to violate basic rules of arithmetic.[88] Judge Sentelle perhaps put it best in his dissent from the D.C. Circuit's denial of the Government's petition for rehearing en banc in *Jones* when he pointed out that "[t]he sum of an infinite number of zero-value parts is also zero."[89] Although a bit punchy in the presentation, the conceptual issue is clear enough.

The problem that Judge Sentelle identifies is not merely mathematical. It also highlights the mosaic theory's apparent absence of Fourth Amendment pedigree and its potential tensions with mainstays of Fourth Amendment doctrine and analysis. For example, most searches are the result of what might be described as evolving encounters. That is, officers develop reasonable suspicion or probable cause through a series of investigative steps and interactions with suspects.[90] As Orin Kerr has pointed out, the Court's Fourth Amendment jurisprudence has always taken a synchronic rather than diachronic approach when evaluating the reasonableness of law enforcement conduct during these evolving encounters.[91] The Court's recent decision in *Kentucky v. King*[92] provides a ready example.

> 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.

Id. at 562.

[88] An additive mathematical identity, in this case zero, does not change the number to which it is added. *Additive Identity*, MERRIAM WEBSTER DICTIONARY ONLINE, http://www.merriam-webster.com/dictionary/additive%20identity (last visited Jan. 23, 2013).

[89] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle J., dissenting); *see also Jones*, 132 S. Ct. at 954 ("The concurrence posits that 'relatively short-term monitoring of a person's movements on public streets' is okay, but that 'the use of longer term GPS monitoring in investigations of *most offenses*' is not good. That introduces yet another novelty into our jurisprudence." (citations omitted)).

[90] One court explained "evolving encounters" as a situation "where new facts continually emerge . . . justifying police action that only moments before would have been unlawful." People v. Sloup, 834 N.E.2d 995, 1000 (Ill. App. 2005).

[91] Kerr, *supra* note 32, at 314–19, 337.

[92] 131 S. Ct. 1849 (2011).

In *King*, police officers followed a suspect, who had just purchased crack cocaine from an undercover agent, into an apartment building.[93] As they entered the building's breezeway, they heard a door close, but could not discern which of two apartments the suspect had entered.[94] The officers had no reason to think that the suspect knew he was being followed, so they had no claim of hot pursuit or any other emergency at that point.[95] They did, however, detect the smell of burning marijuana emanating from behind one door, so they decided to knock, announce themselves, and request entry.[96] The predictable ensued. Immediately after announcing their presence, the officers heard noises inside the apartment that might reasonably have indicated that evidence was being destroyed.[97] Based on that suspicion, the officers forced the door open and entered the apartment.[98] Once inside, the officers seized several people on the scene, conducted a *Buie*[99] protective sweep, and in the course of that search found marijuana, cocaine, drug paraphernalia, and cash in plain view.[100] As it turned out, the initial suspect was not in the apartment, but three other people were, including the eventual respondent: Hollis King.[101]

King was convicted on several narcotics charges and appealed to the Supreme Court of Kentucky.[102] Although skeptical that the sounds officers heard coming from the apartment were enough to justify an unwarranted entry under the emergency exception to the

---

[93] *Id.* at 1854.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] Maryland v. Buie, 494 U.S. 325, 335–36 (1990) ("The sweep lasts no longer than is necessary to dispel the reasonable suspicion of danger [to the officers] and in any event no longer than it takes to complete the arrest and depart the premises.").
[100] *King*, 131 S. Ct. at 1854.
[101] *Id.*
[102] *Id.* at 1855.

warrant clause, the Kentucky court assumed as much.[103] It nevertheless held that King's conviction should be vacated because the officers created the emergency.[104] In that court's view, it was unreasonable from a Fourth Amendment perspective for officers to knock on the apartment door because it was foreseeable, given the circumstances, that doing so would create an emergency.[105] The U.S. Supreme Court reversed.[106] In doing so, it rejected approaches adopted in lower courts that required assessing the reasonableness of law enforcement conduct holistically by looking at the totality of an evolving encounter that eventually resulted in a search or arrest.[107] The Court instead recommitted itself to assessing the reasonableness of officer conduct at each step of an encounter.[108] The Court therefore held that all the Fourth Amendment requires is that, at each stage of an evolving investigation or engagement, officers limit themselves to conduct that is reasonable based on what they know or observe.[109] In so holding, the Court reaffirmed its longstanding commitment[110] to an objective and synchronic assessment of Fourth Amendment reasonableness.

The mosaic theory raises serious concerns when considered in the light of cases like *King*. Beyond the mathematical challenge of adding nothings to get something, the very idea of an additive or holistic approach to evaluating Fourth Amendment reasonableness runs contrary to the synchronic approach that is a foundation of long-standing Fourth Amendment analysis.

---

[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.* at 1864.
[107] *Id.* at 1858–61 (describing and rejecting tests based on assessments of "bad faith" and reasonable foreseeability that law enforcement conduct leading to an emergency).
[108] *Id.* at 1863–64.
[109] *Id.*
[110] *See* Kerr, *supra* note 32, 320–43 (explaining the development and application of the synchronic approach to Fourth Amendment cases).

B. *Doctrinal Objections to the Mosaic Theory*

The mosaic theory endorsed by the U.S. Court of Appeals for the District of Columbia and a majority of concurring Justices in *United States v. Jones* proposes nothing short of a revolution in Fourth Amendment law. Never before has the Court suggested that we can have reasonable expectations of privacy in certain quantities or aggregations of information even if we have no such expectations in the constituent parts.[111] As with any doctrinal revolution, the mosaic theory appears to require some blood on the floor. Specifically, adopting a mosaic approach to the Fourth Amendment may require abandoning or dramatically altering two important lines of Fourth Amendment law: the public observation doctrine[112] and the third party doctrine.[113] To the extent that this is so, commitments to these doctrines, or simply to stare decisis, counsel caution before adopting a mosaic theory of Fourth Amendment privacy.

Adopting a mosaic approach to quantitative privacy seems to require abandoning the public observation doctrine, which is often credited to the Supreme Court's decision in *United States v. Knotts*.[114] In *Knotts*, the Court held that using a beeper device to track a suspect's car on public streets did not constitute a "search" because the suspect lacked a reasonable expectation of privacy in

---

[111] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting).

[112] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that an individual has no reasonable expectation of privacy when traveling in public places).

[113] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citations omitted)); United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012) (citing the Government's argument that the mosaic theory as applied to surveillance will hamper police investigations).

[114] *Jones*, 132 S. Ct. at 953 ("This Court has to date not deviated from the understanding that mere visual observation does not constitute a search."); *see also Knotts*, 460 U.S. at 281 ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

his public movements.[115] Although the beeper allowed officers to follow Knotts more efficiently and with fewer personnel, the *Knotts* Court specifically declined to hold that using technology raises any independent Fourth Amendment concerns simply because it makes it easier for law enforcement officers to conduct surveillance that they are otherwise entitled to do using traditional means.[116]

The parallels between *Knotts* and *Jones* are obvious. In both cases, law enforcement officers used a passive signaling device attached to a car.[117] In both cases, the devices revealed only movements on public streets.[118] In both cases, those movements were exposed to public view.[119] Given these similarities, *Knotts* would seem to control in a case like *Jones*, thus barring Fourth Amendment review of GPS-enabled tracking so long as the technology is only used to monitor movements in public.[120] Should the Court eventually adopt a mosaic approach to assessing and protecting quantitative privacy, it would therefore seem obliged to overrule or modify *Knotts* and the long line of subsequent cases[121] endorsing investigative-surveillance techniques and technologies

---

[115] *Knotts*, 460 U.S. at 281.

[116] *Id.* at 284–85.

[117] *Id.* at 277 ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."); *Jones*, 132 S. Ct. at 947 ("By means of signals from multiple satellites, the [GPS] device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer.").

[118] *Jones*, 132 S. Ct. at 950; *Knotts*, 460 U.S. at 281.

[119] *See Jones*, 132 S. Ct. at 950; *Knotts*, 460 U.S. at 281.

[120] United States v. Jones, 625 F.3d 766, 768 (D.C. Cir. 2010) (Sentelle, J., dissenting); *id.* at 769–70 (Kavanaugh, J., dissenting).

[121] *See, e.g.*, Florida v. Riley, 488 U.S. 445 (1998) (holding that anything visible at four hundred feet in the air is open to public view); California v. Greenwood, 486 U.S. 35 (1988) (holding that garbage cans left out for collection is open to public rummaging); California v. Ciraolo, 476 U.S. 207 (1986) (holding that anything visible from public airspace is open to public view).

that merely document what targets knowingly expose to public view.[122]

Among the most compelling examples of these potential disruptions is the effect of the mosaic theory on traditional human surveillance.[123] Visual surveillance is a mainstay of targeted police investigations. Police officers routinely conduct "stake-outs," sometimes using teams of officers and vehicles to track suspects as they move through public spaces.[124] Law enforcement agencies also aggregate information from informants to develop detailed accounts of suspects' public movements.[125] These practices are not only commonplace,[126] they have been routinely endorsed by courts

---

[122] *Jones*, 625 F.3d at 769 (Sentelle, J., dissenting) ("Nowhere in *Knotts* or any other Supreme Court Fourth Amendment decision since the adoption of the expectation of privacy rationale in *Katz* has the Court ever suggested that the test of the reasonable expectation is in any way related to the intent of the user of the data obtained by the surveillance or other alleged search.").

[123] *Id.* at 769 ("Therefore, it would appear, as appellee argues, that this novel aggregation approach to the reasonable expectation of privacy would prohibit not only GPS-augmented surveillance, but any other police surveillance of sufficient length to support consolidation of data into the sort of pattern or mosaic contemplated by the panel. . . . I cannot discern any distinction."); Kerr, *supra* note 32, at 335 ("If the police send a team of investigators to place the suspect under visual surveillance, should that visual surveillance be subject to the same [mosaic] analysis?").

[124] *See* LAWRENCE F. TRAVIS III, INTRODUCTION TO CRIMINAL JUSTICE 179 (Anderson Publishing, 7th ed. 2012) ("The bulk of surveillance conducted by police agencies is physical surveillance."); Sarah Stillman, *The Throwaways*, THE NEW YORKER (Sept. 3, 2012), http://www.newyorker.com/reporting/2012/09/03/120903fa_fact_stillman#ixzz2J3ZyPWC7 ("By some estimates, up to eighty per cent of all drug cases in America involve [informants]"); *see* sources cited *supra* note 126 and accompanying text.; *cf.* 3 COMPREHENSIVE HANDBOOK OF SOCIAL WORK AND SOCIAL WELFARE 228–29 (Karen M. Sowers et al. eds., 2008) (concluding that the use of multiple informants is "the most effective strategy . . . to gather assessment data about a child").

[125] *See, e.g.*, United States v. Jewell, 60 F.3d 20, 23 (1st Cir. 1995) (finding that the combined information of three confidential informants along with other surveillance was sufficient probable cause to obtain a search warrant for the home of a suspected drug dealer); *see also* State v. McCain, 713 S.E.2d 21, 28 (N.C. Ct. App. 2011) (holding that multiple "informants, citizens and anonymous callers" provided enough probable cause for a search warrant).

[126] *See* sources cited *supra* note 124.

as well within Fourth Amendment bounds[127]—a view that is shared even among mosaic promoters[128]—because they document conduct and movements in which the suspect or target has no reasonable expectation of privacy.[129] The mosaic theory puts these practices and the line of doctrine endorsing them in obvious jeopardy, particularly when officers are too successful and their investigations produce too much information.[130] How, after all, are we to distinguish "between the supposed invasion by aggregation of data between the GPS-augmented surveillance and a purely visual surveillance of substantial length"?[131]

In addition to the public observation doctrine, the mosaic theory also threatens to unsettle the "third party doctrine."[132] The Court has long held that citizens who share information with others assume the risk that what they share might be passed along to law enforcement.[133] Applying this rule, the Court has held that there is no Fourth Amendment violation if a criminal confederate shares

---

[127] *See, e.g.*, sources cited *supra* note 125.

[128] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.").

[129] *See, e.g.*, United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945 ("Surveillance that reveals only what is already exposed to the public—such as a person's movements during a single journey—is not a search.") (citing United States v. Knotts, 460 U.S. 276, 285 (1983)).

[130] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting).

[131] *Id.* As we shall see below, one important mosaic defender resolves this apparent tension by submitting all surveillance, whether manual or technologically-enhanced, to the same time constraints. *See infra* Part IV.C.

[132] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 526 (2006) ("This doctrine provides that if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information.").

[133] *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[A citizen] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." (citations omitted)).

the confidences of his co-conspirators with police,[134] if a bank shares a customer's financial records with law enforcement,[135] or if a telephone company discloses records of phone calls customers make or receive.[136] More recently, a New York court ruled that a customer of the social networking website Twitter[137] had no standing to challenge a lawful subpoena issued against the company for locational information embedded in his posts because he voluntarily shared that information with Twitter.[138]

As Justice Sotomayor, who expresses sympathy for some version of the mosaic theory in her *Jones* concurrence, points out, "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[139] That is because we routinely share vast quantities of data with private agents, many of whom store it.[140] Our Internet service providers track and keep detailed records of where we go on the internet.[141] Our chosen search engines

---

[134] *See* Hoffa v. United States, 385 U.S. 293, 299–302 (1966) (holding that there was no Fourth Amendment violation of privacy when a co-conspirator told police about plans to bribe jury members).

[135] Cal. Banker's Ass'n v. Shultz, 416 U.S. 21, 67–69 (1974). Congress responded to decisions like *Miller* and *Shultz* by passing the Right to Financial Privacy Act of 1978, 29 U.S.C. §§ 3401–3422 (2006), which provides bank customers some privacy regarding their records held by banks and other financial institutions and stipulates procedures whereby federal agencies can gain access to those records.

[136] Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that a person who uses a phone "assume[s] the risk that the [telephone] company [will] reveal to the police the numbers he dialed"). The Pen Register Act attempted to fill the void left by *Smith v. Maryland* by requiring a court order to use a pen register or trap and trace device. Electronic Communications Privacy Act of 1986 § 301(a), 18 U.S.C. § 3121(a) (2001)*; see also* DANIEL J. SOLOVE, THE DIGITAL PERSON 205 (2004) ("Whereas a pen register records the telephone numbers a person dials from her home, a trap and trace device creates a list of the telephone numbers of incoming calls.").

[137] TWITTER, https://twitter.com. (last visited Feb. 20, 2013).

[138] People v. Harris, 945 N.Y.S.2d 505, 507–10 (N.Y. Crim. Ct. 2012).

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

[140] *See* Slobogin, *supra* note 19, at 7; Citron, *supra* note 14.

[141] *See* Citron, *supra* note 21.

gather information not only on our search patterns, but also where we go, what we look at, and what stimuli we react to while online.[142] For most of us, law enforcement would not need to install GPS-enabled devices on our persons or cars if they wanted to track us in the same way that officers tracked the defendants in *Jones* because we already carry GPS chips in our telephones, cars, and computers that pass along information about our movements to a wide range of third parties, from map services to social network applications and restaurant rating sites.[143] Moreover, these third parties are already in the habit of sharing much of the information they gather. Data brokers aggregate and analyze vast reservoirs of data from financial institutions, retailers, public records, social networking sites, and just about anywhere we interact with the physical or virtual worlds.[144] The third party doctrine provides the Government with unfettered access to all of this data[145]—so much so that Chris Hoofnagle has coined the phrase "Big Brother's Little Helpers" to describe data brokers like Acxiom,[146] which aggregate data from public and third-party sources to compile detailed mosaics of information on anyone and everyone.[147]

As Justice Alito suggested in his *Jones* concurrence, most of this information sharing is motivated by an interest in

---

[142] *See* Declan McCullagh, *FAQ: Protecting Yourself from Search Engines*, CNET (Aug. 8, 2006), http://news.cnet.com/FAQ-Protecting-yourself-from-search-engines/2100-1025_3-6103486.html.

[143] *See* Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 493, 528 (2012) ("Precise, persistent cell phone tracking also provides considerably more information: it reveals a person's location at all times, not just when he or she is driving.").

[144] *See generally* U.S. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (explaining the Commission's recommendations to companies for increased consumer privacy).

[145] *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1451 (2011).

[146] ACXIOM, http://www.acxiom.com (last visited Jan. 22, 2013).

[147] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595 (2004).

convenience.[148] We readily embrace "[n]ew technolog[ies] [that] may provide increased convenience or security at the expense of privacy."[149] Having done so, the third party doctrine instructs us that there is no violation of reasonable expectations of privacy if the Government gains access to personal information through those with whom we have shared it. Proponents of the mosaic approach to quantitative privacy resist this result, but in doing so appear obliged to modify or overturn the third party doctrine.[150] This would not only mean a break with long-established doctrine, but would also throw into doubt a wide range of common investigative techniques, notably the use of confidential informants, accessing credit histories, and confirming residential histories.

C. *Practical Concerns with the Mosaic Theory*

Many of the conceptual and doctrinal issues outlined in the foregoing sections lead to serious practical concerns that critics on and off the courts have argued should urge us to caution before adopting the mosaic theory of Fourth Amendment privacy. The most crucial is that translating the mosaic theory into practice will mean drawing important lines between aggregations of information that trigger reasonable expectations of privacy and those that do not.[151] Justice Scalia identifies the challenges in *Jones*. As he puts the point, mosaic advocates are on the hook for a coherent, practical, and doctrinally acceptable test that explains why short-term monitoring is allowed but "a 4-week investigation is 'surely' too long."[152] In an early commentary on *Jones*, Orin Kerr echoed Justice Scalia's concerns, asking, "How long must the tool be used

---

[148] United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

[149] *Id.*

[150] *See, e.g.*, Slobogin, *supra* note 19, at 16–17; *cf.* Kerr, *supra* note 32, at 332 (using third-party data collection to illustrate the difficulty in determining when the mosaic theory will apply to information gathering).

[151] *Jones*, 132 S. Ct. at 954; Kerr, *supra* note 32, at 330–31 (claiming that the mosaic theory lacks a clear standard).

[152] *Jones*, 132 S. Ct. at 954. For further discussion of *Knotts*, see *supra* notes 51–56, 115–122, and accompanying text. Gray & Citron, *supra* note 34, meets this challenge.

before the relevant mosaic is created?"[153] As Kerr has further pointed out, this line-drawing problem extends past mosaics constructed using a single investigative method, as was the case in *Jones*,[154] to include investigative portfolios aggregated using a variety of methods, perhaps including human surveillance.[155]

There is no doubt that this line-drawing problem is serious. Among the most important burdens of any Fourth Amendment standard is that it must provide clear guidance to police officers and lower courts.[156] Muddy and unpredictable tests are both unfair and ultimately fail to provide substantial protection.[157] From a more theoretical perspective, failure to provide fair warning may, as Lon Fuller has argued, constitute a failure to make law in the first place.[158] This failure to adequately make law ultimately compromises the goal of protecting rights. After all, if law enforcement officers cannot predict with certainty whether investigative programs implicate the Fourth Amendment, then they are that much more likely to routinely, if unintentionally, violate

---

[153] *See* Kerr, *supra* note 32, at 330–33.

[154] *Jones*, 132 S. Ct. at 946.

[155] *See* Kerr, *supra* note 32, at 334.

[156] *See id.* at 331–32 (explaining the uncertainty created under the mosaic theory as to when in the course of a surveillance a search occurs).

[157] *See* Dunaway v. New York, 442 U.S. 200, 213–14 (1979) ("A single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront."); United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting) (arguing that the mosaic theory does not produce predictable results); *see, e.g.*, United States v. Robinson, 414 U.S. 218, 235 (1973) (declaring that searching an arrested person is reasonable under the 4th Amendment); *see also* Thornton v. United States, 541 U.S. 615, 622–23 (2004) ("The need for a clear rule, readily understood by police officers and not depending on differing estimates of what items were or were not within reach of an arrestee at any particular moment, justifies the sort of generalization which *Belton* enunciated."). *But see* Ohio v. Robinette, 519 U.S. 33, 34 (1996) (reflecting that the Court has "consistently eschewed bright-line rules, instead emphasizing the fact-specific nature of the reasonableness inquiry").

[158] *See* LON FULLER, THE MORALITY OF LAW 33–39 (2d ed. 1964).

the very reasonable expectations of privacy that the mosaic theory seeks to identify and protect.[159]

Troublesome in their own right, these line-drawing problems also raise serious concerns that the mosaic theory would dramatically skew the balance of interests urged by the Fourth Amendment.[160] At base, Fourth Amendment reasonableness requires protecting both the legitimate interests of law enforcement officers and the privacy interests of citizens.[161] As the Court has often indicated, providing officers with clear rules of conduct preserves this balance by erecting important privacy protections and by preserving adequate space for aggressive law enforcement.[162] Some commentators have suggested that the very vagueness of the mosaic theory threatens to paralyze law enforcement officers in the midst of active investigations because they will be forced to worry constantly whether their efforts have been so successful that they have created a mosaic, implicating the Fourth Amendment.[163]

Assuming that mosaic advocates can meet line drawing concerns, downstream issues of application remain. For example, should investigations that could potentially create mosaics be bound by the warrant requirement, or will it be enough for officers to justify their conduct retrospectively?[164] If a warrant is not required, what level of suspicion is necessary to justify investigations that might generate mosaics?[165] Is reasonable suspicion sufficient, or is probable cause required?[166] Should there be different standards for different investigative techniques or

---

[159] *See* Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468–69 (1985).

[160] *Jones*, 625 F.3d at 767–68 (Sentelle, C.J., dissenting) (arguing that the aggregation technique of the mosaic theory would impede previously acceptable police investigation techniques).

[161] *See infra* note 223 and accompanying text.

[162] *See, e.g.*, *Dunaway*, 442 U.S. at 213–14; *cf.* Slobogin, *supra* note 19, at 5.

[163] *See, e.g.*, Kerr, *supra* note 32, at 331–32, 347–50.

[164] *Id.* at 338.

[165] *See id.*

[166] *Id.*

mosaics of different form, nature, or dimension?[167] Then there is the question of remedy. As the Court has made clear, a Fourth Amendment violation does not determine the remedy.[168] Should the exclusionary rule govern mosaic violations?[169] If so, will it be effective given the likelihood that many mosaic violations will be the result of investigations pursued in good faith that are simply more successful retrospectively than law enforcement thought they would be ex ante?[170] For its detractors, the mosaic theory simply creates too many questions and not enough answers to become a rule of force in Fourth Amendment law.

IV. DEFENDING THE MOSAIC THEORY

Mosaic advocates have not been silent in the face of objections and concerns advanced by the theory's critics. To the contrary, they have both met the objections and developed concrete proposals meant to address many of these concerns. This Part reviews some of those efforts, suggests other possible responses, and offers assessments of their success.

A. *Responding to Conceptual Objections*

Among the most nettlesome of conceptual objections to the mosaic theory is Judge Sentelle's premise that "[t]he sum of an infinite number of zero-value parts is also zero."[171] If *Knotts* was correctly decided, and we do not have reasonable expectations of privacy in our public movements, then we cannot, by *modus tollens* and within the rules of arithmetic, have a reasonable

---

[167] *Id.* at 338–39.

[168] *See* Davis v. United States, 131 S. Ct. 2419, 2427 (2011) ("For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs."); United States v. Herring, 555 U.S. 135, 140 (2009) ("The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies." (quoting Illinois v. Gates, 462 U.S. 213, 223 (1983)).

[169] *See* Kerr, *supra* note 32, at 340.

[170] *Id.* at 341.

[171] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting).

expectation of privacy in any aggregated collection of our public movements.

Mosaic advocates appear to respond that the critique misunderstands the point. Reasonable expectations of privacy, they contend, are not theoretical.[172] Rather, they are practical assessments of common social practices and expectations.[173] Thus, as Judge Ginsburg explains, it is both possible and likely that a "passerby" might "observe or even follow someone during a single journey as he goes to the market or returns home from work."[174] We are all familiar with such happenstances, and at one point or another have found ourselves driving the same roads with a fellow traveler for miles and hours, or perhaps even briefly following someone who looks vaguely familiar to determine whether they are, in fact, that person on whom we had a crush in the eighth grade. By contrast, Judge Ginsburg points out, "the likelihood that a stranger would observe all [of 'a person's movements over the course of a month'] is not just remote, it is essentially nil."[175] Cast in this practical light, Judge Sentelle's conceptual criticism seems to have little traction on the mosaic theory because the atomic-molecular distinction between individual bits of data and large aggregations of data proposed by the mosaic theory is grounded in autoethnography[176] and practical realities rather than ontology.

---

[172] United States v. Maynard, 615 F.3d 544, 559–60 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012) (citing Bond v. United States, 529 U.S. 334 (2000) (discussing practical social expectations regarding the touching and manipulation of bags on a passenger bus); Florida v. Riley, 488 U.S. 445 (1998) (discussing practical social expectations regarding flight in public airspace); California v. Greenwood, 486 U.S. 35 (1988) (discussing practical social expectations regarding the contents of garbage cans left out for collection); and California v. Ciraolo, 476 U.S. 207 (1986) (discussing practical social expectations regarding flight in public airspace)).

[173] *Maynard*, 615 F.3d at 559–560.

[174] *Id.* at 560.

[175] *Id.*

[176] Autoethnographic research focuses on "analyz[ing] personal experience in order to study cultural experience." Carolyn Ellis, Tony Adams & Arthur Bochner, *Autoethnography: An Overview*, 12 FORUM QUALITATIVE SOZIALFORSCHUNG / FORUM: QUALITATIVE SOC. RES. 1 (2011).

Although tempting in some ways, this purely practical approach to defending the mosaic theory probably does not provide much of a safe harbor. The reason why is evident from the Court's holding in *United States v. Kyllo*.[177] There, the Court was asked whether the use of a heat detection device "to explore details of the home that would previously have been unknowable without physical intrusion" constituted a Fourth Amendment search.[178] Writing for the Court, Justice Scalia held that it did, in part because the device in question was "not in general public use."[179] The implication, of course, is that if heat detection devices became ubiquitous features of smartphone cameras, such that any member of the public could observe heat emanations from a home, then police officers would be entitled to do the same without implicating the Fourth Amendment. There could no longer be a reasonable expectation of privacy in those emanations from a descriptive, ethnographic point of view if the technology were to become ubiquitous.

Although heat detection devices remain relatively rare,[180] the same is not true for GPS-enabled tracking devices or data aggregation technologies. Quite to the contrary, GPS chips are in "general public use" in our cellular phones, cars, computers, and tablets.[181] Private purchases of GPS-enabled tracking devices are also on the rise as the technology becomes cheaper and easier to use.[182] As a consequence, for most of us, the aggregate of our daily

---

[177] 533 U.S. 26 (2001).

[178] *Id.* at 40.

[179] *Id.*

[180] A recent search for thermal imaging devices revealed a price tag between $2,000 and $27,000 per device. *Thermal Imaging Cameras, Thermal Imaging Scopes & More*, OPTICSPLANET.COM, http://www.opticsplanet.com/heat-seekers-termal-imagers.html (last visited Jan. 23, 2013). *But see* Daniel Cooper, *Modder Builds $150 Open-Source Thermal Imaging Camera To Help Insulate His House*, ENGADGET (Sept. 3, 2012), http://www.engadget.com/2012/09/03/iphone-thermal-imaging/ (reporting on a developing $150 thermal imaging app for iPhone and Android devices).

[181] *See* Freiwald, *supra* note 20, at 713–14.

[182] David Joachim, *Devices That Track Every Precious Need*, N.Y. TIMES (Apr. 9, 2008), http://www.nytimes.com/2008/04/09/technology/techspecial/09

movements in public are actually exposed to private parties through the very technology used by law enforcement officers in *Jones*.[183] Given this state of affairs, it is hard to make the case for a mosaic theory of the Fourth Amendment based solely on social expectations to the extent they are a function of common practice. Even if such a case could be made with reference to present realities, it would have little staying power because surveillance and data aggregation technologies will only become more and more endemic over time.[184]

There is another, perhaps more promising, response to Judge Sentelle's mathematical objection. Rather than concede that we have no expectations of privacy at all in the fragments of a mosaic, advocates might argue that we actually do have some reasonable expectations of privacy in our discrete public jaunts, but those meager interests just do not to come anywhere close to outweighing the significant law enforcement interests at stake in observing citizens in public places. Although perhaps in tension with some of the language of cases like *Knotts*,[185] adopting this view would make the arithmetic work. It would also be consistent with the Court's account of the Fourth Amendment as requiring a reasonable balance between law enforcement interests and citizens' privacy interests.[186] Practical problems would remain, of

---

postal.html ("Tracking devices that use the Global Positioning System have become so compact and inexpensive that some people are using them routinely to keep tabs on their most precious things.").

[183] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[184] *See* Orin S. Kerr, *The Case Against the Mosaic Theory*, USVJONES.COM (June 4, 2012), http://usvjones.com/2012/06/04/the-case-against-the-mosaic-theory/ (warning that the mosaic theory cannot respond to changing technologies). Assuming that the mosaic theory could be defended purely by reference to practical expectations, advocates appear to run full force into doctrinal problems, and particularly the problem of human surveillance. *See infra* Part IV.B.

[185] United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

[186] *See* Slobogin, *supra* note 19, at 5.

course,[187] but this account of the mosaic theory appears to resolve the conceptual concern.

By far the most promising response to the argument that the sum of nothings cannot be something, however, is to take seriously the metaphor of the mosaic. It may well be true that the "sum of an infinite number of zero-value parts is also zero,"[188] but mosaic advocates need not and do not make their case based on addition.[189] Quite to the contrary, their key claim is that the "whole" of one's movements in public "reveals more—sometimes a great deal more—than does the sum of its parts."[190] The mosaic theory is, then, not an exercise in arithmetic. Rather, it recognizes that, although a collection of dots is sometimes nothing more than a collection of dots, some collections of dots, when assessed holistically, are *A Sunday Afternoon on the Island of La Grande Jatte*.[191] So, too, are our lives.

As Justice Sotomayor observed in *Jones*, a "precise, comprehensive, record of a person's public movements . . . reflects a wealth of detail about her familial, political, professional, religious and sexual associations."[192] The tapestries of our lives are by definition an aggregation of events and activities that, when assessed discretely, or even iteratively, may have little significance. When assessed holistically, however, these events not only tell a detailed story of our activities and associations, they may reveal who we are at a fundamental level and therefore expose opportunities for manipulation and control. It may not take much. For example, according to one recent study, researchers were able to pierce the veil of anonymity cast over a body of locational data

---

[187] *See supra* Part III.C.

[188] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010).

[189] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (applying the mosaic theory to aggregated surveillance).

[190] *Id.* at 558.

[191] Georges Seurat, *A Sunday on La Grande Jatte – 1884,* ART INST. OF CHI., http://www.artic.edu/aic/collections/artwork/27992?search_id=1&index=0 (last visited Jan. 4, 2013). The painting is an example of pointillism, which is a technique defined by the use of individual dots to create an image. *Id.*

[192] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

and identify particular users by referencing as few as four "spatio-temporal points."[193] The mosaic theory's core claim, then, is not that we have a reasonable expectation of privacy in flashing moments, or even in meaningless arithmetic concatenations of those events. Rather, mosaic theorists argue that we have a reasonable expectation of privacy in the whole of our lives, and therefore have a Fourth Amendment right to be free from constant, indiscriminate, and pervasive surveillance.[194]

Building out from this core, Justice Sotomayor's concurrence in *Jones* supports another important response to the arithmetic objection. Fourth Amendment privacy is not an ethereal abstraction. To the contrary, as a constituent of rights bundled together in the first eight Amendments to the U.S. Constitution,[195] the negative rights afforded by the Fourth Amendment[196] secure the space that is necessary to pursue the blessings of fundamental liberty. As Justice Sotomayor points out, "Awareness that the Government may be watching chills associational and expressive freedoms."[197] Only by providing substantial privacy protections can we truly be at liberty to explore and pursue the good life as we conceive it. Thus, Justice Sotomayor tells us, "GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society."[198]

---

[193] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in a Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REP., Mar. 25, 2013, at 1376, *available at* http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

[194] *See Maynard*, 615 F.3d at 563 (concluding under the mosaic theory that aggregated surveillance is outside the reasonable expectation of privacy).

[195] U.S. CONST. amends. I–VIII.

[196] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

[197] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

[198] *Id.* (internal quotation marks and citation omitted).

Although this holistic account of the mosaic theory may answer Judge Sentelle's mathematical concerns, it appears to run full force into conceptual objections raised by Orin Kerr that the mosaic engages a previously rejected diachronic account of the Fourth Amendment.[199] Here, however, mosaic advocates have a ready response: The objection misunderstands the thesis. Embracing a mosaic approach to assessing Fourth Amendment privacy interests does not require taking an equally holistic view of law enforcement conduct. That is, it may be true that officer conduct during the course of an investigation does not constitute a "search" when assessed discretely, or even in the aggregate, but, nevertheless, may produce a mosaic of personal information that is sufficiently expansive and detailed to implicate reasonable expectations of privacy. There is no doubt that this shift in focus from the conduct of law enforcement to the fruits of their investigative efforts raises serious practical problems when weighing Fourth Amendment interests. After all, officers naturally want to be able to make prospective assessments of whether the Fourth Amendment will apply so they will know how to proceed. For now, however, it seems that a holistic framing of the mosaic theory can meet the major conceptual objections, at least insofar as it is treated as a way to understand Fourth Amendment interests and harms. Whether and how the mosaic theory can be converted into a useful set of practices and policies is a separate matter, which we address below.[200]

B. *Responding to Doctrinal Objections*

As we saw in the preceding section, the most persuasive way to conceptualize the mosaic theory is to focus on what aggregations of data reveal when assessed holistically rather than iteratively or additively. So understood, the mosaic theory seems also to have promising responses to the doctrinal objections discussed in Part III.B.

---

[199] *See* Kerr, *supra* note 32, at 315–20.
[200] *See infra* Part IV.C.

The first doctrinal challenge we saw in Part III came from the public observation doctrine. How, critics wondered, can we square the rule from *Knotts*—that police officers are free to make any observations they care to from a place where they have a lawful right to be—with the proposition that, if officers see *too much*, then the Fourth Amendment is implicated? [201] Here again, advocates might be tempted to lean on Judge Ginsburg's observation that "the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil."[202] As we saw above, however, this line of response actually threatens to maximize rather than minimize doctrinal damage. After all, the chances that any of us is being observed by law enforcement officers at any given time are also "effectively nil."[203] Judge Ginsburg's argument therefore seems to put at risk a host of one-off surveillance practices that are routine for most police officers, even if foreign and unexpected for many of their subjects.

At any rate, Judge Ginsburg's distinction relies on a false premise. Despite our contrary expectations, it is increasingly the case that we are, in fact, being monitored much or most of the time by a combination of law enforcement officers, governmental regulators, and their legions of willing and unwilling private sector

---

[201] *See* United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945 (citing the Government's argument that the mosaic theory as applied to surveillance will hamper police investigations). According to the Government, "[such a proposition] logically would prohibit even visual surveillance of persons or vehicles located in public places and exposed to public view, which clearly is not the law." Brief of Respondent-Appellee at 62, *Maynard*, Nos. 08-3030 and 08-3034 (D.C. Cir. June 8, 2009), 2009 WL 3126569 (citing *United States v. Knotts*, 460 U.S. 276, 282 (1983)).

[202] *Maynard*, 615 F.3d at 558. *See also Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("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 enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

[203] *Maynard*, 615 F.3d at 558.

agents.[204] No matter how honestly held, then, the expectations that Judge Ginsburg cites are, on the whole, not reasonable insofar as reasonable expectations of privacy are indexed to reality.[205]

All of this suggests that recognizing the mosaic theory would require abandoning or significantly modifying the public observation doctrine,[206] and perhaps the *Katz* reasonable expectation of privacy test as well.[207] This is true even if the mosaic theory focuses on the enhanced privacy interests implicated by aggregations of data and information as a whole. First, mosaics that trigger Fourth Amendment concerns can be aggregated in sundry ways, including by using multiple investigative techniques.[208] Without additional guidance, conducting traditional surveillance for a day, a week, or a month might reveal too much. Similarly, a targeted, but short technologically-enhanced investigation might easily reveal enough to cross the threshold. Second, given the increasing ubiquity of what Christopher Slobogin has called "panvasive surveillance,"[209] defending a mosaic theory appears to require treating the *Katz* reasonable expectation of privacy test as proscriptive rather than descriptive. Although attractive to many privacy advocates, that move would

---

[204] *See supra* Part I.

[205] Katz v. United States, 389 U.S. 347 (1967) (holding that electronic monitoring of conversations in public telephone constitutes a "search" under the Fourth Amendment)*; id*. at 353, 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' ").

[206] United States v. Knotts, 460 U.S. 276, 281 (1983); *see also supra* Part III.B (discussing the public observation doctrine and the reduced expectation of privacy while in public).

[207] *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

[208] *See* Kerr, *supra* note 32, at 334 (using *Jones* as an example by recounting that "[t]he government obtained cell phone location records, installed a public surveillance camera, and watched the suspects in public, all in addition to tapping phones and obtaining text messages").

[209] Christopher Slobogin, *Rehnquist and Panvasive Searches*, MISS. L.J. (forthcoming 2013), *available at* http://ssrn.com/abstract=2158935.

dramatically change the Fourth Amendment landscape, potentially reopening questions once thought settled.[210]

The only way for mosaic theorists to avoid falling off this doctrinal cliff is to come forward with a clear evaluative test that law enforcement officers can deploy prospectively to reliably determine which investigative techniques they can employ, and to what extent, before triggering Fourth Amendment requirements. Thus, as we saw in the foregoing discussion of conceptual issues,[211] the focus quickly turns to the practicalities. There is simply no doubt that adopting a mosaic theory of the Fourth Amendment will require modifying the public observation doctrine. How much modification is required, and the type of adjustment needed, will be a function of the test advocates adopt.[212]

In contrast with the inevitable confrontation that mosaic theorists must have with the public observation doctrine, any conflict with the third party doctrine is entirely avoidable. It is by

---

[210] *See, e.g.*, I.N.S. v. Delgado, 466 U.S. 210, 215 (1984) ("The Fourth Amendment does not proscribe all contact between the police and citizens, but is designed to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals." (internal quotation marks omitted)). Examples of previously settled questions that may be affected by a shift to proscriptive analysis include whether a bus passenger has a reasonable expectation of privacy in luggage, whether there is a reasonable expectation of privacy in garbage, and whether a customer has a reasonable expectation of privacy in banking records. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000) ("Thus, a bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here."); *see also* California v. Greenwood, 486 U.S. 35, 40 (1988) ("It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."); United States v. Miller, 425 U.S. 435, 442 (1976) ("The checks are not confidential communications but negotiable instruments to be used in commercial transactions.").

[211] *See supra* Part IV.A.

[212] Elsewhere, the authors propose and defend a "technology centered approach" that resolves these practical problems. *See* Gray & Citron, *supra* note 35.

now settled that the Fourth Amendment binds only state actors.[213] Thus, there is no constitutional barrier to private parties' engaging in surveillance activities that would be subject to Fourth Amendment regulations if conducted by government officials.[214] Justice Sotomayor's suggestion in *Jones* that the Court might need to fundamentally reconsider the third party doctrine if it chooses to embrace the mosaic theory[215] is therefore not motivated by doctrinal necessity. Rather, it reflects practical concerns that the privacy interests and harms identified by the mosaic theory will not be fully vindicated unless private actors are also subject to constraint or government agents are limited in terms of what information they can gather through third parties.

This really involves two concerns. The first is that law enforcement officers will simply circumnavigate the Fourth Amendment by subpoenaing from private parties information that the officers could not gather directly. The second is that informational mosaics in the hands of private parties are no less invasive and objectionable for being in private rather than state hands. In response to both concerns, promoters of the mosaic theory can simply maintain that worries about the absence of practical protections for informational mosaics in light of the third party doctrine are constitutionally gratuitous. They are also not new. Similar arguments have been raised before the Court when it has held the line on the third party doctrine.[216] In most of these

---

[213] *See* United States v. Jacobsen, 466 U.S. 109, 113–14 (1984) (holding that private actors are not bound by the Fourth Amendment unless working as agents of the state).

[214] *See* United States v. Jones, 132 S. Ct. 945, 961 (2012) (Alito, J., concurring) ("By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.").

[215] *Id*. at 957 (Sotomayor, J., concurring).

[216] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979) (ruling that the Fourth Amendment is not implicated when law enforcement places pen registers on numbers called by telephone customers); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 54 (1974) ("[T]he mere maintenance of the records by the banks under the compulsion of the regulations invade[s] no Fourth Amendment right . . . .");

cases, the political branches have responded, imposing legal limitations on the gathering, preservation, and sharing of information from banks,[217] telephone companies,[218] and e-mail providers.[219] The Court is free to exercise the same restraint should it adopt the mosaic theory, and thereby avoid any entanglement with the third party doctrine. Should it choose this more parsimonious path, it would go a long way toward silencing many mosaic critics.[220]

C. *Responding to Practical Concerns*

The foregoing analysis suggests that mosaic theorists have promising, if not always satisfying, responses to most of the conceptual and doctrinal objections that have so far been raised against the mosaic theory of Fourth Amendment privacy. Many of these responses are incomplete, however, in that they put considerable pressure on how the practical details are resolved. Therefore, whether the mosaic theory can provide a foundation for elaborating Fourth Amendment interests in response to developed and developing surveillance technologies is, in large part, a function of how well the mosaic theory can be translated into a set of coherent and workable rules and policies.

United States v. White, 401 U.S. 745 (1971) (refusing to recognize Fourth Amendment violation when private informant secretly taped conversations with defendant).

[217] *See* Bank Secrecy Act of 1970, Pub L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended in scattered sections of 12 and 31 U.S.C.) (requiring banks to maintain secrecy of customer information except in certain circumstances).

[218] *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 3121-27 (2012)) (setting forth requirements for law enforcement to obtain information about telephone communications).

[219] *See id.*

[220] *See* Kerr, *supra* note 32, at 350 (criticizing mosaic theory and arguing that the Court should exercise restraint in order to preserve space for the legislature to regulate contemporary surveillance technologies); Erin Elizabeth Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485 (2013).

As courts put the mosaic theory into practice, the first line of challenges they will need to address are line-drawing problems. How are officers and courts to determine whether a particular informational mosaic contains enough information to implicate Fourth Amendment rights? Does the quality of information in the mosaic come into play, or is it merely the quantity? Does the method of acquisition matter? How are police officers to know, prospectively, whether the Fourth Amendment applies, when, and what it demands? All of these are important questions that ultimately feed back into the various conceptual and doctrinal issues already discussed.

A good place for mosaic advocates to start is by pointing out that these sorts of line-drawing problems are not unique to the mosaic theory. Rather, they are endemic to the Fourth Amendment itself.[221] The animating core of the Fourth Amendment is reasonableness.[222] Reasonableness, in turn, requires a balancing of competing law enforcement and privacy interests.[223] It is therefore no surprise that Fourth Amendment analysis is often more nuanced than it is definitive, or that Fourth Amendment tests tend to describe spectrums rather than bright lines. Take, for example, the Court's approach to probable cause, the threshold requirement that must be met before officers can engage in searches for evidence. Writing for the Court in *Illinois v. Gates*,[224] then-Justice Rehnquist tells us that "probable cause is a . . . practical, nontechnical" standard and is "a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even

---

[221] *See* Coolidge v. New Hampshire, 403 U.S. 443, 474–75 (1971) (finding no surprise and little weight in "the unstartling proposition that when a line is drawn there is often not a great deal of difference between situations closest to it on either side").

[222] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

[223] *See* United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

[224] 462 U.S. 213 (1983).

usefully, reduced to a neat set of legal rules."[225] These are mushy standards indeed, and no doubt produce a range of reasonable, but conflicting, views among courts,[226] not to mention angst in the law enforcement community.[227] Despite these difficulties, the Court has yet to excuse officers or courts from responsibility for "slosh[ing] [their] way through the factbound morass of 'reasonableness.' "[228]

It is hard to see how the line-drawing concerns raised by mosaic critics are any more worrisome than the line-drawing problems that are inherent to the Fourth Amendment.[229] Although adopting the mosaic would likely lead to some growing pains,[230] there is no reason to think that courts and law enforcement officers are incapable of growth. At any rate, fear of adjustment is no reason to leave a constitutional right unprotected, much less unrecognized. Of course, if assessing aggregations of information and investigative procedures under a mosaic theory proves too difficult using the case-by-case, fact-centered approach favored by

---

[225] *Id.* at 231–32.

[226] *See* California v. Acevedo, 500 U.S. 565, 583 (1991) (Scalia, J., concurring) ("I do not regard today's holding as some momentous departure, but rather as merely the continuation of an inconsistent jurisprudence that has been with us for years . . . . There can be no clarity in this area unless we make up our minds, and unless the principles we express comport with the actions we take."); Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 n.3 (1985) (describing United States v. Ross, 655 F.2d 1159, 1160 (D.C. Cir. 1981) *rev'd*, 456 U.S. 798 (1982), a case in which four dissenting judges disagreed as to the appropriate standard for warrantless searches).

[227] *See* Bradley, *supra* note 226, at 1468–69 ("The Court's failure to provide such rules leads not only to the exclusion of evidence in cases involving the guilty, but also to intrusions upon the rights of both the innocent and the guilty by police who, faced with incomprehensibly complex rules either ignore them or, in their efforts to follow them, make mistakes which lead to evidentiary exclusion.").

[228] Scott v. Harris, 550 U.S. 372, 383 (2007).

[229] *See* Jim Harper, *Escaping Fourth Amendment Doctrine After Jones: Physics, Law, and Privacy Protection*, CATO SUP. CT. REV., 2011–2012, at 219, 244, *available at* http://www.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2012/9/scr-2012-harper.pdf (criticizing the "reasonable expectation of privacy test" as overly subjective and confusing to courts).

[230] *See* Kerr, *supra* note 32, at 347.

the Court in other Fourth Amendment circumstances,[231] then there is always the option of drawing bright lines. It would not be the first time. For example, the Court has adopted a bright(ish) line forty-eight-hour rule when assessing the reasonableness of municipal policies governing probable cause hearings after warrantless arrests.[232] It has also excused law enforcement officers from the burden of showing independent probable cause, or any other additional justification, when conducting searches incident to arrest.[233] If it is necessary to do so in order to vindicate Fourth Amendment rights, while avoiding thorny line-drawing problems, the Court could follow a similar course after adopting a mosaic theory.

In some of his recent work, Christopher Slobogin has suggested just such a bright line approach to implementing the mosaic theory.[234] Under his proposal, which is presented as a model statute, any targeted "search"—defined succinctly as an "effort by government to find or discern . . . information about a specific person or circumscribed place" in connection with a known criminal event—would be subject to increasing constraint based on the aggregated time of that search.[235] Specifically, targeted searches, conducted by any means that last longer than

---

[231] *See, e.g.*, Ohio v. Robinette, 519 US 33, 39 (1996) (declining to impose a bright line rule requiring officers to inform suspects that they are free to go before pursuing a consensual interrogation); Michigan v. Chesternut, 486 U.S. 567, 572 (1988) (declining to hold that investigatory pursuits always constitute Fourth Amendment "seizures").

[232] Cnty. of Riverside v. Mclaughlin, 500 U.S. 44, 57 (1991).

[233] Chimel v. California, 395 U.S. 752 (1969) (allowing for a search of a vehicle and the area in which an arrestee might lunge for a weapon). The Court limited the bright line rule announced in *Chimel* in the context of searches of cars incident to arrest. *See* Arizona v. Gant, 556 U.S. 332 (2009); *see also* Thornton v. United States, 541 U.S. 615, 623 (2004) (holding that an officer can search the vehicle that an arrestee recently exited); *cf.* United States v. Ross, 456 U.S. 798, 824 (1982) ("The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found.")

[234] *See* Slobogin, *supra* note 19, at 16.

[235] *Id.* at 17.

forty-eight hours in the aggregate, would require a warrant;[236] searches that last between twenty minutes and forty-eight hours in the aggregate would require a court order;[237] and searches that last fewer than twenty minutes in the aggregate would only require some good faith basis.[238] Targeted data searches, whether conducted directly or through third parties, would be subject to similar time constraints, with forty-eight hours again marking the trigger point for the warrant requirement.[239]

The great virtue of Professor Slobogin's proposal, as with other bright line approaches, is its clarity and ease of application. That clarity comes with costs, of course, along some of the conceptual and doctrinal dimensions discussed above. For example, Professor Slobogin's proposal runs full-force into doctrinal concerns based on *Knotts*. In particular, he draws no distinction between human surveillance and technologically enhanced surveillance.[240] Any court that adopted his approach would therefore need to effect pretty dramatic modifications to the public observation doctrine up to, and likely including, overturning *Knotts*. After all, the surveillance in *Knotts* lasted longer than twenty minutes,[241] which under Professor Slobogin's proposal would require a court order.[242]

A court adopting Professor Slobogin's approach would also find itself confronted with conceptual and doctrinal objections based on the traditional synchronic approach to evaluating the Fourth Amendment reasonableness of law enforcement conduct.[243] That is because Professor Slobogin chooses duration of surveillance as the metric for measuring Fourth Amendment trigger points.[244] Additionally, he assesses surveillance time

---

[236] *Id.* at 25.
[237] *Id.*
[238] *Id.*
[239] *Id.* at 28.
[240] *Id.* at 19.
[241] United States v. Knotts, 460 U.S. 276, 277–80 (1983).
[242] *See* Slobogin, *supra* note 19, at 25.
[243] *See supra* Part III.A. (describing the objections).
[244] *See* Slobogin, *supra* note 19, at 26 ("Rules based on duration are easier to understand and abide by. While precise time divisions such as those used in this provision are arbitrary in the sense that they apply regardless of how intrusive

inclusively,[245] which also requires taking a diachronic, rather than synchronic, view of law enforcement conduct.

Another difficulty with bright line approaches such as the one Professor Slobogin describes is that, ironically enough, they often ignore the actual mosaics of information aggregated by officers during a challenged investigation. As a consequence, bright lines draw boundaries that are both over-inclusive and under-inclusive. For example, with the benefit of sophisticated statistical analysis, officers may be able to develop very revealing mosaics of personal information by spot sampling personal data and GPS-enabled tracking information.[246] As long as the aggregate of that sampling does not add up to more than twenty minutes, however, there would be no Fourth Amendment regulation if duration of surveillance was used to describe the Fourth Amendment boundary.[247] The same can be said for short-term, but potentially revelatory, use of discrete surveillance technologies like drones.[248] Contrariwise, rather lengthy and unproductive human surveillance

---

the search actually is, time limitations as a method of defining constitutional protections have a solid pedigree.").

[245] *Id.* at 25.

[246] *See* Kerr, *supra* note 32, at 333 (discussing GPS software that can take information at specific intervals). It is entirely within the realm of possibility that police will soon have access to software that can cross-reference locational data with other records, such as credit cards, which would give further insight into a suspect's actions. *Cf.* Josh Constine, *Facebook Beta Launches New Mobile Ad Network Using Your Data to Target You with Banner Ads in Other Apps*, TECHCRUNCH (Sept. 18, 2012), http://techcrunch.com/2012/09/18/facebook-mobile-ad-network/ (explaining Facebook's plan to merge off-site ads with biographical, locational, and social information provided by Facebook users for a more targeted advertising system).

[247] *See* Susan Freiwald, *The Four Factor Test*, USVJONES.COM (June 4, 2012), http://usvjones.com/2012/06/04/the-four-factor-test/ (finding the Alito concurrence in Jones an incomplete solution).

[248] *See* Marc Blitz, United States v. Jones – *and the Forms of Surveillance That May Be Left Unregulated in a Free Society*, USVJONES.COM (June 4, 2012), http://usvjones.com/2012/06/04/united-states-v-jones-and-the-forms-of-surveillance-that-may-be-left-unregulated-in-a-free-society/ (arguing that focusing only on long-term surveillance is an inadequate constitutional protection).

would require a warrant,[249] even if it ultimately produced nothing close to the sort of informational mosaics that worried the concurring Justices in *Jones*.

None of this is meant to condemn Professor Slobogin's proposal, of course. Rather, the point is that, precisely because solutions for the conceptual and doctrinal challenges to the mosaic lean so heavily on the practicalities of implementation, any approach that is adopted will have conceptual and doctrinal consequences.[250] The upshot is that compromises, conflict, and adjustment are inevitable. As with all Fourth Amendment questions, the test of success will be whether efforts to implement the mosaic theory can accomplish a reasonable balance between law enforcement goals and privacy interests.[251] Reaching that balance has been a constant struggle since 1791.[252] There is no reason to hope or expect that it will be any simpler in the coming years as advocates and critics work through the potential and consequences of a mosaic theory of Fourth Amendment privacy.

V. CONCLUSION

This Article has attempted to advance debates after *United States v. Jones* about the conceptual, doctrinal, and practical issues that attend the mosaic theory of Fourth Amendment privacy. The discussion has not produced a clear conclusion. Rather, the goal has been to elaborate the major objections raised against the mosaic theory to provide guidance for mosaic advocates. Although it is beyond the scope of the present Article to advance a

---

[249] *See* Slobogin, *supra* note 19, at 27–28.

[250] *See id.* at 36.

[251] *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."); *supra* note 156 and accompanying text.

[252] The Bill of Rights, including the Fourth Amendment, was first ratified in 1791. *See* 2 HOWARD GILLMAN, MARK A. GRABER, & KEITH E. WHITTINGTON, AMERICAN CONSTITUTIONALISM 81 (2013); *see* M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. REV. 905, 907–19 (2010) (outlining the history of the Fourth Amendment and how this history has informed its interpretation).

mosaic-based proposal, the core insights that drive the theory warrant that further development.[253] At its core, the mosaic theory documents perfectly reasonable expectations that we will not be forced to live in a surveillance state or to abide constant, indiscriminate surveillance conducted by the Government or its private proxies.[254] That this expectation has firm footing in the Fourth Amendment we take to be a proposition that is constitutionally unproblematic.[255] The devil may well be in the details, but to the extent the mosaic theory is understood as a way to conceptualize these privacy interests and corollary privacy harms, the game is well worth the candle.

[253] The authors develop and defend our own positive proposal elsewhere. *See, e.g.*, Gray & Citron, *The Right to Quantitative Privacy*, *supra* note 36.

[254] *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

[255] *See* Slobogin, *supra* note 19, at 12.