2018

Fourth Amendment Constraints on the Technological Monitoring of Convicted Sex Offenders

Ben A. McJunkin
University of Michigan Law School

J. J. Prescott
University of Michigan Law School, jprescott@umich.edu

FOURTH AMENDMENT CONSTRAINTS ON THE TECHNOLOGICAL MONITORING OF CONVICTED SEX OFFENDERS

Ben A. McJunkin and J.J. Prescott***

More than forty U.S. states currently track at least some of their convicted sex offenders using GPS devices. Many offenders will be monitored for life. The burdens and expense of living indefinitely under constant technological monitoring have been well documented, but most commentators have assumed that these burdens were of no constitutional moment because states have characterized such surveillance as "civil" in character—and courts have seemed to agree. In 2015, however, the Supreme Court decided in Grady v. North Carolina *that attaching a GPS monitoring device to a person was a Fourth Amendment search, notwithstanding the ostensibly civil character of the surveillance.* Grady *left open the question whether the search—and the state's technological monitoring program more generally—was constitutionally reasonable. This Essay considers the doctrine and theory of Fourth Amendment reasonableness as it applies to both current and envisioned sex offender monitoring technologies to evaluate whether the Fourth Amendment may serve as an effective check on post-release monitoring regimes.*

Keywords: *Fourth Amendment, sex offenders, monitoring, GPS technology, search, privacy, post-release regulations*

*Alumni Fellow, University of Michigan Law School.

**Professor of Law, University of Michigan Law School. We are very grateful to Daniel Ruiz for his thoughtful engagement with us on this project. We also thank Eve Brensike Primus, Evan Caminker, and Wayne Logan for helpful comments on an earlier draft.

New Criminal Law Review, Vol. 21, Number 3, pps 379–425. ISSN 1933-4192, electronic ISSN 1933-4206. DOI: https://doi.org/10.1525/nclr.2018.21.3.379.

INTRODUCTION

The technological monitoring of sex offenders is not a new phenomenon.[1] It has, however, become an increasingly popular one. Laws subjecting convicted sex offenders to some form of technological monitoring, often for very long terms or lifetimes, have multiplied in the past decade.[2] Rapid technological advancements now permit relatively low-cost location tracking twenty-four hours per day, seven days per week.[3] Some legal scholars have lauded these developments because technological monitoring of sex offenders appears to impose "minimal intrusion" compared to alternative forms of social control.[4] Yet that claim has rarely been examined in detail. In fact, courts have largely assumed that the intrusion imposed by technological monitoring was insufficiently serious to warrant constitutional scrutiny.[5] That is, until the Supreme Court upset this easy assumption.

---

1. *See* Avlana K. Eisenberg, *Mass Monitoring*, 90 S. CAL. L. REV. 123, 146–48 (2017) (documenting the development and expansion of sex offender monitoring dating back many years). Throughout this Essay, we use the term "technological monitoring" (and variants of this term) to refer not only to the variety of location-based tracking authorized by current sex offender laws—including satellite-based Global Positioning System (GPS) devices and radio frequency (RF) transmitters—but also more broadly to any deployment of current or future technology in a manner that permits individualized tracking and observation.

2. See discussion *infra* Part I.

3. Further, under many state statutes, the costs of maintaining technological monitoring are passed on to the offender subject to monitoring. *See, e.g.*, Rhonda Cook, *Sex Offender Argues Mandatory Ankle Monitors Are Unconstitutional*, THE ATL. J.-CONST. (Dec. 5, 2016), https://www.myajc.com/news/local/sex-offender-argues-mandatory-ankle-monitors-are-unconstitutional/SaXCToWMJ3wgmFm2mvMuzN/.

4. *See* Pamela Foohey, *Applying the Lessons of GPS Monitoring of Batterers to Sex Offenders*, 43 HARV. C.R.-C.L. L. REV. 281, 284 (2008). Although our observations here are focused on the monitoring of sex offenders, the future of criminal justice is likely to include increased technological monitoring in lieu of punishment. *See, e.g.*, Mirko Bagaric, Dan Hunter, & Gabrielle Wolf, *Technological Incarceration and the End of the Prison Crisis*, 108 J. CRIM. L. & CRIMINOLOGY 73, 77 (2018) (proposing technological and remote surveillance as a substitute for physical incarceration). The insights of this Essay therefore may have extended applicability, both for litigants fighting for less intrusive monitoring laws and for legal actors and institutions wishing to monitor individuals in a constitutional manner.

5. Constitutional challenges to sex offender monitoring programs—historically mounted under legal frameworks, such as the Ex Post Facto Clause, the Due Process Clause of the Fourteenth Amendment, and the Eighth Amendment, that do not treat the intrusiveness of monitoring as doctrinally salient—have typically been unsuccessful. *See* Nicholas Corsaro,

In March 2015, the Supreme Court held in *Grady v. North Carolina* that attaching a device to a person's body to track their movements, without consent, is a search subject to judicial review for reasonableness under the Fourth Amendment.[6] The Court declined to decide the question whether North Carolina's monitoring requirement was reasonable. But it did offer general guidance to lower courts reviewing monitoring programs: "The reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations."[7] *Grady* thus provides a new constitutional lens for analyzing sex offender monitoring programs, one that explicitly invites examination of the intrusion experienced by the individual through application of the Fourth Amendment's long-standing search-and-seizure principles.

This Essay proceeds in four parts. Part I provides an overview of the substance and diversity of current laws authorizing the technological monitoring of convicted sex offenders. It situates these monitoring regimes within the rapid historical development of laws regulating convicted sex offenders more generally—such as sex offender registries, reporting and notification requirements, and inclusion and exclusion zones. It also discusses the well-documented burdens and disabilities that technological monitoring imposes on those subject to surveillance. Part II reports the recent developments in the Supreme Court's Fourth Amendment jurisprudence that have opened the door for new legal challenges to the intrusion of technological monitoring. It examines both the *Grady* decision and its predicate case, *United States v. Jones*, which unsettled the conventional understanding of when governmental use of technological monitoring qualifies as a search. It also explains the framework for resolving the ultimate question of the constitutionality of sex offender monitoring laws—whether the monitoring, as a search, is "unreasonable."

Note, *Sex, Gadgets, and the Constitution—A Look at the Massachusetts Sex Offender GPS-Tracking Statute*, 48 SUFFOLK L. REV. 401, 414–19 (2015).

6. *Grady*, 135 S. Ct. 1368, 1371 (2015). The law at issue in *Grady* created a satellite-based monitoring program that maintained time-correlated and continuous tracking of the geographic location of the subject and required reporting of subject's violations of prescriptive and proscriptive schedule or location requirements. *See* N.C. GEN. STAT. ANN. § 14-208. 40(c) (West 2017).

7. *Grady*, 135 S. Ct. at 1371.

Part III is the heart of the Essay. It identifies and explores several distinct dimensions along which the technological monitoring of sex offenders may be considered especially intrusive. It links the identified dimensions of intrusion to both existing Fourth Amendment doctrines and contemporary scholarly theories about the Amendment's future. In so doing, it highlights several pressure points, where the implementation of technological monitoring regimes for sex offenders may need to be curtailed or tailored to accommodate longstanding interests protected by the Fourth Amendment, such as privacy, bodily integrity, and human dignity. Part IV picks up where Part III ends, anticipating and evaluating two theoretical avenues that governments who seek to legislate around the Fourth Amendment might explore, concluding that such attempts would be limited in their efficacy.

Ultimately, this Essay asks a simple, but fundamental question: To what extent does the Fourth Amendment actually constrain whether and how monitoring technologies can be used to surveil sex offenders (or even criminal offenders more broadly)? In answering that question, we seek to accomplish two goals. First, we aim to inform and educate legal actors who have a vested interest in ensuring the constitutionality and reasonableness of sex offender monitoring laws, whether they are legislators designing monitoring regimes for the benefit of their constituents or litigants seeking to find a way out from under particularly invasive monitoring requirements. Second, we interject ourselves into this discrete moment of constitutional uncertainty to help ensure that open foundational questions of Fourth Amendment jurisprudence are resolved thoughtfully and conscientiously, despite arising in a context—the regulation of convicted sex offenders—that can spur strong emotions and lead to hasty conclusions.

I. THE STATE OF SEX OFFENDER MONITORING

Sometime near the start of the twenty-first century, states began to use technology to monitor formerly incarcerated sex offenders.[8] Florida,

8. *See* Eisenberg, *supra* note 1, at 147–48; Eric M. Dante, Comment, *Tracking the Constitution—The Proliferation and Legality of Sex-Offender GPS-Tracking Statutes*, 42 Seton Hall L. Rev. 1169, 1169 (2012); Associated Press, *States Track Sex Offenders by GPS*, Wired (July 30, 2005), https://www.wired.com/2005/07/states-track-sex-offenders-by-gps/.

California, and Massachusetts led the way.[9] By 2006, more than twenty states monitored sex offenders with technological devices.[10] As of 2015, the number of states had grown to more than forty.[11] The statutory basis for sex offender monitoring varies from state to state. Some states, such as Wisconsin and North Carolina, make it available upon a convicted sex offender's release from civil commitment.[12] Other states, such as California and Alaska, make it a condition of parole or probation.[13] At least one state, Michigan, imposes sex offender monitoring as part of the sentence imposed at conviction for a number of specified sex offenses.[14]

Technological monitoring programs for sex offenders differ on other fronts, too. In pointing this out, we are not about to embark on presenting a complete picture of monitoring regimes in the United States. We will instead simply offer a few examples to highlight how much variation there is along different dimensions. One example is whether monitoring is discretionary. In some states, the decisions whether and how to impose monitoring require an individualized assessment from a neutral decision-maker.[15] Depending on the state, this may be either a judge or a parole board.[16] In other states, at least for certain offenses, monitoring is mandatory.[17] Similar diversity exists with respect to the duration of technological

---

9. Dante, *supra* note 8, at 1172.

10. NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE CRIME LEGISLATION IN 2006, 1–2 (2007), http://www.ncsl.org/print/cj/2006crime.pdf.

11. Dante, *supra* note 8, at 1172; Richard Wolf, *High Court Orders Review of Sex Offender GPS Monitoring*, USA TODAY (Mar. 30, 2015), https://www.usatoday.com/story/news/nation/2015/03/30/supreme-court-sex-offender-gps/70544348/.

12. *See, e.g.*, WIS. STAT. § 301.48 (2010); N.C. GEN. STAT. § 14-208.30B.

13. *See, e.g.*, ALASKA STAT. § 12.55.100(f) (2017); CAL. PENAL CODE § 3004 (West 2012).

14. *See* MICH. COMP. LAWS § 750.520n(1) (2006).

15. *See, e.g.*, CONN. GEN. STAT. § 53a-30(a)(14) (2017) (permitting judges to impose monitoring); MISS. CODE. ANN. § 99-19-84 (2014) (permitting judges to impose GPS monitoring as condition of parole); N.J. STAT. ANN. § 30:4-123.91(c) (West 2007) (permitting judges complete discretion as to imposing monitoring on certain sex offenders); N.Y. PENAL LAW § 65.10(4) (McKinney 2010) (permitting court to impose monitoring when it will "advance public safety.").

16. *See, e.g.*, TENN. CODE ANN. § 40-39-302(b)(1) (2014) (granted parole board authority to impose monitoring); WASH. REV. CODE § 9.94A.704(5) (2016) (permitting Department of Corrections to impose monitoring).

17. *See, e.g.*, CAL. PENAL CODE § 3004(b) (2012); FLA. STAT. § 948.30 (2016); GA. CODE ANN. § 42-1-14(e) (2016); MD. CODE ANN., CRIM. PROC. § 11-723(c)(1)(i), (d)(3)(i) (2017); MASS. GEN. LAWS ch. 265 § 47; MICH. COMP. LAWS 750.520n(1) (2006); MO. REV. STAT. §

monitoring. At least seven states, at least for certain crimes, require monitoring for life.[18]

Technological monitoring numbers among a broad gamut of laws regulating convicted sex offenders. Legislation aimed specifically at sex offenders dates as far back as the 1930s, when many states passed laws permitting the indefinite civil commitment of "sexual psychopaths."[19] In the 1990s, a new wave of civil commitment laws—this time styled as "sexual predator" laws—gained momentum, committing offenders in addition to (not in lieu of) their prison terms.[20] Legal regulations governing post-release sex offenders rapidly proliferated following Congress's passage of the Jacob Wetterling Crimes Against Children and Sexually Violent Offenders Registration Act in 1994, which required states to generate registries of convicted sex offenders.[21] Within a few years, every state had its own sex offender registration law. Registries were soon followed by community notification laws, conventionally known as Megan's Law,[22] which made these registries public. Before long, residency, employment, and travel restrictions were added to the list.[23]

Constitutional challenges to the legal regulation of sex offenders have met with little overall success. In 1997, the Supreme Court upheld Kansas's civil commitment statute, concluding that the law comported with due process, did not subject the offender to double jeopardy, and was not an ex

---

217.735 (2017); N.C. GEN. STAT. § 14-208.40, 208.40A(c) (2017); R.I. GEN. LAWS § 11-37-8.2.1 (2006); WIS. STAT. § 301.48 (2011).

18. Corsaro, *supra* note 5, at 412; *see, e.g.*, CAL. PENAL CODE § 3004(b) (2012); GA. CODE ANN. § 42-1-14(e) (2016); MD. CODE ANN., Crim. Proc. § 11-723(c)(1)(i), (d)(3)(i) (2017); MICH. COMP. LAWS § 750.520n(1) (2006); MO. REV. STAT. § 217.735 (2017); N.C. GEN. STAT. § 14-208.40, 208.40A(c) (2017); R.I. GEN. LAWS § 11-37-8.2.1 (2006); WIS. STAT. § 301.48 (2011).

19. *See, e.g.*, Roxanne Lieb et al., *Sexual Predators and Social Policy*, 23 CRIME & JUST. 43, 55 (1998); Raquel Blacher, Comment, *Historical Perspective of the "Sex Psychopath" Statute: From the Revolutionary Era to the Present Federal Crime Bill*, 46 MERCER L. REV. 889, 897 (1995).

20. Corsaro, *supra* note 5, at 404.

21. 42 U.S.C. § 14071.

22. The laws are so named because Congressional support for sex offender registration was spurred by the death of Megan Kanka at the hands of a convicted child molester. *See* Smith v. Doe, 538 U.S. 84, 89 (2003) (explaining that Kanka's death inspired legislative action).

23. *See* J.J. Prescott, *Portmanteau Ascendant: Post-Release Regulations and Sex Offender Recidivism*, 48 CONN. L. REV. 1035, 1038 (2016).

post facto punishment.[24] In 2003, the Court similarly rejected an ex post facto challenge to Alaska's sex offender registration and community notification laws, and a due process challenge to Connecticut's online sex offender registry.[25] Although a few state supreme courts, federal district courts, and federal courts of appeal have struck down particularly onerous or vague sex offender registration, notification, and residency restriction laws in recent years, most courts remain unmoved.[26] In large part, laws regulating sex offenders have been insulated from constitutional scrutiny by their ostensibly "civil" character, notwithstanding their clear ties to issues of crime and punishment.[27] Legal challenges to the technological monitoring of sex offenders are only just beginning to percolate through the courts, but to date, these have not shown much promise of altering this trend.[28]

II. SEARCHING SEX OFFENDERS

Historically, the Fourth Amendment has not offered purchase for push-back to laws regulating convicted sex offenders.[29] However, a "quiet revolution" in Fourth Amendment law may reveal hitherto unrealized constraints on the permissible scope of technological monitoring of convicted sex offenders.[30] This Part outlines the current state of Fourth Amendment law as it pertains to sex offender monitoring regimes. It traces the re-emergence of the so-called "trespass" test for identifying whether

24. Kansas v. Hendricks, 521 U.S. 346, 371 (1997).

25. *Smith*, 538 U.S. at 105–06; Conn. Dept. of Pub. Safety v. Doe, 538 U.S. 1, 8 (2003).

26. *See* Wayne A. Logan, *Challenging the Punitiveness of "New Generation" SORN Laws* (in this Issue).

27. Eisenberg, *supra* note 1, at 161–66.

28. Doe v. Bredesen, 507 F.3d 998, 1000 (6th Cir. 2007) (upholding Tennessee's sex offender monitoring statute in the face of another ex post facto claim).

29. *See, e.g.*, Doe v. Cuomo, 755 F.3d 105, 115 (2d Cir. 2014) (rejecting Fourth Amendment challenge to sex offender registration act); Doe v. Shurtleff, 628 F.3d 1217, 1226–27 (10th Cir. 2010) (rejecting Fourth Amendment challenge to requirement that registered sex offenders provide state with online identifiers and passwords); Roe v. Marcotte, 193 F.3d 72, 79–80 (2d Cir. 1999) (rejecting Fourth Amendment challenge to creation of sex offender DNA data bank).

30. *See* Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward A Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. L. REV. 103, 104 (2017).

particular governmental conduct effects a search, the development that laid the groundwork for extending Fourth Amendment protections to technological monitoring of sex offenders. It then outlines the "reasonableness" framework for assessing whether a given search—and ultimately a state's sex offender monitoring scheme—is constitutional. Using a recent decision from the Seventh Circuit Court of Appeals as a lens, it concludes by highlighting the range of governmental interests likely to hold sway with courts that must be weighed against the intrusiveness of a given monitoring regime.

A. Property and Privacy: Reorienting the Fourth Amendment Inquiry

For most of the last fifty years, the arc of Fourth Amendment search jurisprudence was thought to be linear. The text of the Fourth Amendment secures "persons, houses, papers, and effects" against searches and seizures that are unreasonable.[31] Consistent with that text, early Fourth Amendment protections largely tracked private property rights—a "search" occurred when the government physically invaded a constitutionally protected space.[32] In the late 1960s, however, *Katz v. United States* signaled a sea change in constitutional search analysis. Declaring that "the Constitution protects people, not places," the *Katz* Court announced that a search occurs whenever a citizen's reasonable expectation of privacy is violated, regardless of whether the invasion attended a physical trespass.[33] In the conventional telling of this story, the "reasonable expectation of privacy" test that emerged from *Katz* was an evolution (or perhaps revolution) that replaced the classic trespass doctrine and reoriented the Fourth

31. U.S. CONST. amend. IV.

32. *Compare* Olmstead v. United States, 277 U.S. 438, 457, 464 (1928) (holding that no Fourth Amendment "search" occurred where the government tapped telephone wires outside of a suspect's premises), *and* Goldman v. United States, 316 U.S. 129, 134–35 (1942) (holding that no Fourth Amendment "search" occurred where the government placed a recording device against the outer wall of a suspect's office), *with* Silverman v. United States, 365 U.S. 505, 511 (1961) (holding that a Fourth Amendment "search" occurred when the government inserted a microphone into a suspect's wall because that action constituted a legal trespass).

33. Katz v. United States, 389 U.S. 347, 353 (1967) ("We conclude that . . . the 'trespass' doctrine . . . can no longer be regarded as controlling. . . . The fact that the electronic devices employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").

Amendment around notions of privacy rather than property.[34] In the decades following *Katz*, many other traditional Fourth Amendment doctrines were similarly recast in the language of privacy.[35]

The Supreme Court's 2012 decision in *United States v. Jones*, however, unsettled this account of Fourth Amendment search jurisprudence. Writing for a majority of the Court, Justice Scalia proclaimed that *Katz*'s reasonable expectation of privacy test "has been *added to,* not *substituted for*, the common-law trespassory test."[36] Ironically, the impetus for resuscitating the decades-old trespass doctrine was the government's deployment of modern monitoring technology. In *Jones*, federal agents had secretly installed a GPS tracking device on the defendant's vehicle without a valid warrant to do so.[37] Under the Supreme Court's historical precedents, the information collected by the GPS device—the movement of an automobile on public roads—was arguably not private.[38] Thus, the government's actions were unlikely to run afoul of the *Katz* test, barring some novel proclamation from the Court about the quantum of information gathered or the technological means employed.[39] Instead, the *Jones* Court

34. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 67–68 (2013).

35. For example, the Supreme Court had long held that no Fourth Amendment "search" occurs when police investigate open fields because of an old common law distinction between open fields and houses, only the latter of which are explicitly protected by the Fourth Amendment. *See* Hester v. United States, 265 U.S. 57, 59 (1924). Following *Katz*, the Supreme Court has couched the same result in the rhetoric of privacy, holding that "an individual may not legitimately demand privacy for activities conducted out of doors in fields." Oliver v. United States, 466 U.S. 170, 178 (1984).

36. *Jones*, 565 U.S. 400, 409 (2012). Throughout this Essay, we occasionally refer to the rule articulated in *Jones*, as Justice Scalia did, as a "trespass" test. While we find this a useful shorthand, the Supreme Court's Fourth Amendment jurisprudence both before and since *Jones* evidences that the test does not require an actual trespass, in the legal sense, but rather a physical occupation of a private space. *See generally* Kerr, *supra* note 34.

37. *See Jones*, 565 U.S. at 402–03.

38. *See* 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."). The District Court in *Jones* had suppressed any GPS data collected while vehicle was parked in a private garage. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part on other grounds sub nom.* United States v. Jones, 565 U.S. 400 (2012).

39. Supreme Court commentators had anticipated that the case would be a test of the "mosaic" theory of Fourth Amendment searches, which holds that the aggregation of large

ruled that the installation of the GPS device itself was a Fourth Amendment search, irrespective of the privacy of the information collected.[40] Emphasizing that the government "physically occupied private property for the purpose of obtaining information," Justice Scalia reasoned that the Fourth Amendment must, at a minimum, provide today's citizens with the same protection against trespassory governmental surveillance that it afforded at the time it was adopted.[41] In its next Term, the Court again eschewed the *Katz* test in a Fourth Amendment case, emphasizing instead the "physical intrusion" involved in a police dog search of the curtilage of a home.[42]

Jones set the stage for the Supreme Court's 2015 decision in *Grady v. North Carolina*.[43] The *Grady* case involved a challenge to a North Carolina statute imposing satellite-based monitoring on recidivist sex offenders.[44] By authority of the statute, Dale Grady was ordered to wear a monitoring device at all times for the rest of his life.[45] The state courts had rejected Grady's claims that the monitoring was an unconstitutional search or seizure, reasoning that the lessons of *Jones* did not extend into a non-investigative context—North Carolina's monitoring program was civil in nature, and its purported aim was not the collection of evidence but rather the deterrence of future

---

quantities of erstwhile non-private information may violate a reasonable expectation of privacy. *See* Orin Kerr, *Supreme Court Agrees to Review Case on GPS and the Fourth Amendment*, VOLOKH CONSPIRACY (June 27, 2011), http://volokh.com/2011/06/27/supreme-court-agrees-to-review-case-on-gps-and-the-fourth-amendment/. For more on the mosaic theory, see discussion *infra* Part III.B.

40. *Jones*, 565 U.S. at 402, 411–12.

41. *Id.* at 404–05, 411. *See also id.* at 414 (Sotomayor, J., concurring) (describing the trespass test as "an irreducible constitutional minimum"). The commitment to preserving historical levels of constitutional protection in the face of emerging technology has been championed in recent years by Professor Orin Kerr. *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011). Previously, a similar sentiment had been advanced by Professor Geoffrey Stone. *See* Geoffrey R. Stone, *The Scope of the Fourth Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers*, 1976 AM. B. FOUND. RES. J. 1193 (1976). For counterarguments, see David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 233–41 (2015).

42. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

43. *Grady*, 135 S. Ct. 1368 (2015).

44. *Id.* at 1369. *See generally* N.C. GEN. STAT. ANN. §§ 14–208.40(a)(1), 14–208.40B (2013).

45. *Grady*, 135 S. Ct. at 1369.

crimes.[46] The Supreme Court, however, rejected those distinctions, reminding the courts below (and the rest of us) that the Fourth Amendment has a long history governing civil searches for purposes other than the collection of criminal evidence.[47] In a per curium opinion, the *Grady* Court announced simply that the North Carolina monitoring program involves a Fourth Amendment search because it "is plainly designed to obtain information" and "does so by physically intruding on a subject's body."[48]

The consensus lesson of *Jones* (and *Grady*) is that the nonconsensual, physical occupation of "persons, houses, papers, and effects" for the purpose of collecting information triggers Fourth Amendment scrutiny, separate and apart from any claim to the privacy of the information that results from that occupation.[49] But this is at most a half-victory for those concerned about limiting the potential excesses of technological governmental surveillance. After all, the Fourth Amendment prohibits only *unreasonable* searches.[50] Although *Jones* and *Grady* both held that a "search" had occurred, and thus that each governmental effort was subject to the strictures of the Fourth Amendment, both cases left open the question whether those searches were unreasonable (and hence constitutionally impermissible). The *Jones* Court concluded that the government had waived its argument that GPS monitoring was reasonable by failing to raise it in the Court of Appeals.[51] The *Grady* Court, meanwhile, expressly declined to analyze the reasonableness of North Carolina's satellite-based monitoring of sex offenders regime in the first instance, punting the issue to the state courts.[52]

---

46. *See* State v. Grady, 759 S.E.2d 712 (N.C. App. 2014) (relying on State v. Jones, 750 S. E.2d 883 (2013)); *see also Grady*, 135 S. Ct. at 1371 (noting that "the North Carolina Court of Appeals apparently placed decisive weight on the fact that the State's monitoring program is civil in nature").

47. *Grady*, 135 S. Ct. at 1371.

48. *Id.*

49. *See, e.g.*, William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1834 (2016) ("Justice Scalia's opinion for the Court concluded that the Fourth Amendment protects against trespass-like acts, that a physical intrusion was a trespass-like act, and that affixing the GPS device to the car was a physical intrusion."); Brennan-Marquez & Tutt, *supra* note 30, at 115–16 ("Trespass searches violate the Fourth Amendment even if they infringe on no expectations of privacy at all.").

50. U.S. CONST. amend. IV.

51. United States v. Jones, 565 U.S. 400, 413 (2012).

52. *Grady*, 135 S. Ct. at 1371. On remand, the Court of Appeals of North Carolina recently concluded that the state failed to show that the search was reasonable, both with respect to

It is the half-victory that *Grady* represents that makes this a key constitutional moment for previously incarcerated sex offender monitoring laws. By announcing that the current forms of technological monitoring of sex offenders effects a Fourth Amendment search, without passing judgment on the ultimate constitutional question of reasonableness, the Supreme Court sowed considerable uncertainty on a civil liberties question of major importance.

B. "Unreasonable" Searches: Governmental Interests and Citizen Intrusion

For much of the last century, the Supreme Court seemingly embraced what has been termed the "warrant preference" view of the Fourth Amendment.[53] Although the text of the Fourth Amendment does not state precisely when a search warrant is required,[54] the Supreme Court has repeatedly proclaimed that searches conducted without a warrant—or, at the very least, outside of a judicial process involving prior approval by a judge or a magistrate—are *per se* unreasonable, "subject only to a few specifically established and well-delineated exceptions."[55] This is where scholars well-versed in criminal procedure are likely to chuckle. In application, the "specifically established and well-delineated" exceptions

---

the state's specific interest in monitoring Grady and with respect to the efficacy of its offender monitoring program more generally. State v. Grady, No. COA17-12, 2018 WL 2206344, at *7 (N.C. Ct. App. May 15, 2018).

53. *See, e.g.*, Almeida-Sanchez v. United States, 413 U.S. 266, 277 (1973) (Powell, J., concurring) ("But it is by now axiomatic that the Fourth Amendment's proscription of 'unreasonable searches and seizures' is to be read in conjunction with its command that 'no Warrants shall issue, but upon probable cause.'"). *See also generally* Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133 (2012).

54. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2173 (2016) (citing California v. Acevedo, 500 U.S. 565, 581 (1991) (Scalia, J., concurring in judgment) ("What [the text] explicitly states regarding warrants is by way of limitation upon their issuance rather than requirement of their use.")); Nikolaus Williams, Note, *The Supreme Court's Ahistorical Reasonableness Approach to the Fourth Amendment*, 89 N.Y.U. L. REV. 1522, 1527 (2014) ("The first clause establishes a standard (reasonableness) but does not explain what it means. The second clause states the requirements for a valid warrant but does not explain when warrants are required.").

55. City of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015).

abound.[56] They can be found where the government's interests are substantial,[57] time-bound,[58] or unique;[59] or where the comparative intrusion on privacy is slight,[60] fleeting,[61] or experienced by those who are deemed to have a reduced expectation of privacy from the outset.[62]

Increasingly, the Supreme Court has allowed this view to give up the ghost. In recent years, the Court has proclaimed that reasonableness is the "ultimate touchstone" of Fourth Amendment analysis, and it has begun to perform explicitly that comparison of interests that it had historically engaged in subtextually.[63] Although there are many different formulations of the reasonableness standard, the constitutionality of a warrantless search ultimately turns on an all-things-considered comparison of the government's legitimate interests against the intrusiveness of the search for those subject to it.[64] This is a key development with respect to sex offender monitoring regimes, which may not fall neatly into established categorical exceptions and yet are not ordinarily supported by a warrant and probable cause.[65] In fact, in *Grady* itself, despite the absence of a warrant, the

---

56. *See, e.g.*, Dana Raigrodski, *Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment*, 17 TEX. J. WOMEN & L. 153, 170 (2008) (identifying "some twenty exceptions including searches incident to arrest, automobile searches, stop and frisk searches, plain view searches, consent searches, border searches, administrative searches of regulated businesses, exigent circumstances, welfare searches, inventory searches, airport searches, school searches, searches of mobile homes, and searches of offices of public employees").

57. *See, e.g.*, Michigan v. Tyler, 436 U.S. 499, 509 (1978) (exigent circumstances).

58. *See, e.g.*, United States v. Santana, 427 U.S. 38, 42–43 (1973) (hot pursuit).

59. *See, e.g.*, City of Ontario v. Quon, 560 U.S. 746, 760–66 (2010) (holding that a warrantless search was reasonable due to the special needs of the workplace environment).

60. *See, e.g.*, *Birchfield*, 136 S. Ct. at 2178 (roadside breathalyzer).

61. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (stop and frisk).

62. *See, e.g.*, Samson v. California, 547 U.S. 843, 850–55 (2006) (holding that a warrantless, suspicionless search of parolee was permissible because of parolee's diminished expectation of privacy and government's substantial interest in supervising parolees).

63. *See* Kentucky v. King, 563 U.S. 452, 459 (2011).

64. *Quon*, 560 U.S. at 761 (explaining that searches must be reasonably related to a legitimate interest and not excessively intrusive in light of the circumstances giving rise to the search).

65. Prior to the Supreme Court's recent turn toward a general "reasonableness" standard, the most likely Fourth Amendment doctrinal avenue for assessing the technological monitoring of convicted sex offenders who are "off paper" (i.e., not on probation or parole) would have been the "special needs" doctrine, which permits so-called suspicionless "administrative searches" in service of goals other than law enforcement. *See generally*

Supreme Court remanded the case with an explicit directive for the North Carolina Supreme Court to consider "the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations."[66]

Although Fourth Amendment reasonableness is a holistic evaluation, we are fortunate to have a few guideposts. A reasonable warrantless search typically must be tailored to its aims with roughly the same level of specificity as would be authorized by a valid warrant.[67] The means by which a search is conducted should therefore be "reasonably related in scope to the circumstances which justified the interference in the first place."[68] It is worth emphasizing the word "circumstances" and keeping in mind that each instance of monitoring is a distinct and separate search. In the context of the technological monitoring of convicted sex offenders, this means that the requisite balance is not merely between the governmental interests that justify a monitoring program broadly and the extent of the intrusion experienced by an individual offender.[69] Rather, "as the Court has repeatedly recognized, the *means* of surveillance, the nature of the technology at

---

Skinner v. Ry. Labor Exec.'s Assn., 489 U.S. 602 (1989) (upholding suspicionless drug testing for railroad workers). The special needs doctrine is a questionable fit given that at least some of the interests served by sex offender monitoring statutes are the specific deterrence of the offender and the collection of evidence in the event that deterrence is unsuccessful. *Cf.* Indianapolis v. Edmond, 531 U.S. 32, 43 (2000) (noting that the Court is "particularly reluctant" to find special needs "where governmental authorities primarily pursue their general crime control ends"). For the Fourth Amendment rights of sex offenders on probation or parole, see discussion *infra* Part IV.B.

66. *Grady*, 135 S. Ct. at 1371. Because challenges to sex offender monitoring laws like the one at issue in *Grady* are most likely to brought in federal court under 42 U.S.C. § 1983, this raises the specter of so-called "double reasonableness": the substantive constitutional violation requires that the search be unreasonable, while the availability of remedy turns on a separate assessment of the reasonableness of the violation. *See generally* Sam Kamin & Justin Marceau, *Double Reasonableness and the Fourth Amendment*, 68 U. MIAMI L. REV. 589 (2014).

67. Chimel v. California, 395 U.S. 752, 762–63 (1969).

68. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (articulating a two-step test to measure the reasonableness of a search).

69. Of course, the individualized assessment of technological monitoring also carries the potential to *enlarge* the government's interests with respect to certain offenders (e.g., those with demonstrably high recidivism rates) relative to those interests that justify monitoring at a programmatic level.

issue, and its potential for abuse must be considered as well."[70] Various critical facets of each search, therefore, play a role in the reasonableness determination.

Since *Grady* was decided in 2015, only one federal circuit court has resolved a Fourth Amendment challenge to the technological monitoring of sex offenders. The majority opinion in that case, *Belleau v. Wall*,[71] exemplifies the strong weight courts are inclined to assign to the government's interest in implementing technological monitoring programs against formerly incarcerated people. Writing for a panel of the Seventh Circuit that unanimously declared the monitoring program constitutional, Judge Posner emphasized that Wisconsin's statute worked "to deter future offenses by making the plaintiff aware that he is being monitored and is likely therefore to be apprehended should a sex crime be reported at a time, and a location, at which he is present."[72] Underscoring the gravity of the need for deterrence, Posner dedicated no less than six well-sourced paragraphs of his opinion to the rampant underreporting of sex crimes and to the impact that underreporting has on recidivism statistics, seeking to dispel any hint that the offender in the case might "be thought just a harmless old guy."[73] As a seemingly final nail in the coffin, Posner invited "[r]eaders of this opinion who are parents of young children [to] ask themselves whether they should worry that there are people in their community who have 'only' a 16 percent or an 8 percent probability of molesting young children—bearing in mind the lifelong psychological scars that such molestation frequently inflicts."[74]

Where Judge Posner's opinion falls short, however, is in assessing the intrusion that Wisconsin's technological monitoring statute imposes on offenders. Speaking of the ankle monitor technology challenged in the case, Posner noted in passing that "such devices are also used by some

---

70. Priscilla J. Smith et al., *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177, 182 (2011).

71. *Belleau*, 811 F.3d 929 (7th Cir. 2016).

72. *Id.* at 935.

73. *See id.* at 933–34.

74. *Id.* We do not comment (here) on whether this representation of the risk sex offenders pose to communities is accurate. For our purposes, we assume that at least some sex offenders do pose an elevated risk and therefore there is at least some governmental interest in passing and enforcing post-release sex offender laws that seek to lower this risk.

parents to keep track of their kids or elderly relatives and by some hikers and mountain climbers to make sure they know where they are at all times or to track their speed."[75] Later, he characterized having to wear the monitor as "a bother, an inconvenience, an annoyance," but nothing more.[76] He further insisted that, since the plaintiff's name and address were already on the public sex offender registry, there was little "additional loss [of privacy] from the fact that occasionally his trouser leg hitches up and reveals an anklet monitor that may cause someone who spots it to guess that this is a person who has committed a sex crime."[77] Displaying an oddly anachronistic understanding of surveillance, Posner juxtaposed a lifetime of 24/7 GPS monitoring, which "just identifies locations," with "serious" privacy violations, such as "if the Department of Corrections were following the plaintiff around, peeking through his bedroom window, trailing him as he walks to the drug store or the local Starbucks, videotaping his every move, and through such snooping learning . . . 'whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband,' etc."[78]

That Judge Posner seemed dismissive of the privacy intrusions experienced by a sex offender—one whom he repeatedly labeled as "pedophile," as if to remind the reader of his diminished worth—is hardly surprising. Convicted sex offenders are rarely sympathetic, and tend to arouse anger and disgust in the public.[79] However, the Supreme Court has repeatedly admonished that even the most pressing governmental interests cannot act as a license for indiscriminate police behavior.[80] As the remainder of this Essay demonstrates, the imposition of technological

---

75. *Id.* at 931.

76. *Id.* at 937.

77. *Id.* at 935. We are reminded of Justice Douglas's admonitions in *Osborn v. United States*:

> These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.

385 U.S. 323, 343 (1966) (Douglas, J., dissenting).

78. *Belleau*, 811 F.3d at 935.

79. Prescott, *supra* note 23, at 1041.

80. *See, e.g.*, Maryland v. King, 569 U.S. 435, 447 (2013).

monitoring on sex offenders is no small matter. And, as the wide state-to-state variation in such programs evidences, monitoring is also malleable—it can be implemented in ways that are more or less intrusive and in ways that are more or less tailored to accomplish the government's goals.[81] It is thus an open and evolving question whether and how technological monitoring can be implemented "reasonably," consistent with the security that the Fourth Amendment guarantees to all citizens, regardless of their past crimes.

III. THE DIMENSIONS OF INTRUSION

Notwithstanding the arguably substantial governmental interests at stake in monitoring convicted sex offenders, technological monitoring imposes real and substantial burdens on the individuals subject to it. Proper constitutional analysis requires taking those intrusions seriously.[82] As the Supreme Court has stated, "The gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement may employ to pursue a given purpose."[83] The sections that follow each offer a sketch of the theoretical, doctrinal, and practical arguments that might be advanced with respect to assessing the intrusiveness of technological monitoring as a Fourth Amendment "search." Without purporting to be an exhaustive survey, these sections underscore the variety of dimensions along which offender monitoring programs may potentially be intrusive and which have proven doctrinal relevance under the Fourth Amendment. In practice, measuring the intrusiveness of a search will of course be a heavily fact-bound inquiry, likely turning on the precise technology used, the amount

81. We note that the Supreme Court has at times proven unsympathetic to arguments focused on comparing a challenged search program to less-invasive alternatives. *See, e.g.*, United States v. Martinez-Fuerte, 428 U.S. 543, 556 n.12 (1976) ("The logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers."). We direct the reader to the use of the word "elaborate," however, which would seem to exclude obvious, costless ways to reduce intrusiveness.

82. *See* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

83. City of Indianapolis v. Edmond, 531 U.S. 32, 32–33 (2000).

and nature of information collected, and the specifics of the statute that authorizes the practice. Many of these features, however, can be individualized, tailoring surveillance to offender circumstances, and often entail technologically feasible (although not costless) adjustments that can reduce the burdens of monitoring. By identifying these distinct dimensions of intrusion, our aim is to elucidate the many (and sometimes countervailing) considerations that should inform how the government can conduct technological monitoring in ways that are consistent with Fourth Amendment expectations.[84]

A. Extending the Trespass Test: Physical Invasions

Potentially the most interesting question following *Grady* is also the most unsettled: How heavily does the physical intrusion imposed by a given sex offender monitoring technology weigh in the assessment of whether a search is reasonable? For nearly a half-century, the privacy-centric focus of Fourth Amendment search jurisprudence largely reduced the question of intrusiveness to one of data flows.[85] As a result, case law assessing the intrusiveness of the government's physical invasions under the Fourth Amendment is rare.[86] Further, it is possible that the trespass test articulated in *Jones* will eventually prove to be relevant primarily (or perhaps even

84. In deploying this method, we see our Essay as complementary to the work of notable Fourth Amendment scholars who have isolated and clarified separate strains of jurisprudence that too often fall under a single label. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

85. For a criticism of this state of affairs, see generally David A. Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069 (2014).

86. One such rare exception are Section 1983 civil rights suits claiming that government agents used excessive force (typically when conducting a seizure). *See* Graham v. Connor, 490 U.S. 386, 394–95 (1989) (holding that such claims are properly analyzed under the Fourth Amendment, rather than substantive due process). However, those cases have limited analogical value for evaluating the technological monitoring of sex offenders. They commonly involve the snap judgments of police in the field, rather than programmatic decisions, are bound up with complicated questions of qualified immunity, and primarily surface in the most extreme fact patterns, such as those involving the death of a criminal suspect. *See, e.g.*, Mullenix v. Luna, 136 S. Ct. 305, 310–11 (2015); Anderson v. Creighton, 483 U.S. 635, 638 (1987).

exclusively) to the threshold inquiry of whether a search occurred, rather than to an assessment of that search's reasonableness. We note, for example, that the *Grady* Court itself returned to the language of "reasonable privacy expectations" when it instructed the North Carolina courts to assess the intrusiveness of sex offender monitoring.[87]

We doubt that the *Jones* trespass test can be so cabined, however. The majority opinion in *Jones* turns almost exclusively on the (relatively minor) physical invasion involved in surreptitiously attaching an inconspicuous GPS device to the underside of a vehicle. It was this physical invasion that allowed the *Jones* Court to distinguish two prior precedents in which the Court found that the government's use of technological monitoring to collect similar information did not invade defendants' privacy.[88] *Jones* is thus best read as supporting the commonsense proposition that the *means* of a search matter to whether the search is constitutional[89]: A physical invasion by the government to collect information is a constitutionally significant event, irrespective of the nature of the information it succeeds in collecting.

One useful analog for understanding the weight of physical intrusion in Fourth Amendment analysis came just one year after *Grady*, when the Supreme Court evaluated the reasonableness of two different methods for evaluating the blood-alcohol content of suspected drunk drivers.[90] The Court concluded that a warrantless "breathalyzer" search is reasonable in part because "the physical intrusion is almost negligible."[91] Analogizing the test to

87. Grady v. North Carolina, 135 S. Ct. 1368, 1371 (2015).

88. *See* United States v. Jones, 565 U.S. 400, 409 (reasoning that the prior "beeper" cases did not involve a trespass because the device was installed in the relevant containers prior to the defendant taking possession). *See also* United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S 276 (1983). To be clear, the *Karo* Court held that the government's monitoring of the beeper *did* constitute a Fourth Amendment search once it revealed nonpublic information about the suspect's residence, but not when revealing publicly available information—information such as the location of a vehicle on public roads or the location of a container in an open field. *Karo*, 468 U.S. at 714.

89. Illustrative of the distinction that Justice Scalia was drawing, prior cases were akin to a suspect inviting a wired-up informant into his business (a situation that the Supreme Court has repeatedly found not to be a search), whereas the physical intrusion in *Jones* more closely parallels the surreptitious instillation of a microphone into the wall. *See Jones*, 565 U.S. at 410 (citing On Lee v. United States, 343 U.S. 747, 751–52 (1952)). *See also* Silverman v. United States, 365 U.S. 505, 511 (1961) (holding that a Fourth Amendment "search" occurred when the government inserted a microphone into a suspect's wall).

90. Birchfield v. North Dakota, 136 S. Ct. 2160 (2016).

91. *Id.* at 2176.

drinking out of a straw or blowing up a party balloon, the Court concluded that the search required "nothing painful or strange" of the suspect.[92] The Court, however, struck down compulsory blood tests largely because of the extent of the physical invasion involved, describing the tests as requiring the piercing of the skin to "extract a part of the subject's body."[93] The Court further explained that the blood test's reasonableness "must be judged in light of the availability of the less invasive alternative of a breath test."[94]

Taking a stab at a preliminary framework, we might think of physical intrusion as existing on a spectrum. At one end of this spectrum are "strange or painful" technologies. Although individuals might disagree over the comparative levels of intrusion of specific devices, this end of the spectrum likely includes technologies that require surgical implantation, those that physically implicate portions of the body, and those that cause substantial or long-lasting or chronic pain. At the opposite end of this spectrum would be the least invasive technologies, those akin to simply breathing into a breathalyzer. For example, one can imagine a hypothetical program for sex offender monitoring that requires merely the downloading of a smart phone app and the periodic logging of location through biometric identification on the phone, perhaps by fingerprint or facial recognition technology that is already nearly ubiquitous in American society. Assuming that the trespass rationale of *Jones* and *Grady* would extend to the app's "intrusion" on the smartphone—its occupation of the owner's electronic circuits, stored energy, and memory[95]—the comparative physical

92. *Id.* at 2177. The Supreme Court has likewise upheld the constitutionality of investigative practices like cheek swabs and fingernail scrapings involving only "negligible" or "very limited" physical intrusions. *See King*, 569 U.S. at 446–47; Cupp v. Murphy, 412 U.S. 291, 296 (1973).

93. *Birchfield*, 136 S. Ct. at 2178. The Supreme Court has elsewhere described "compelled surgical intrusion into an individual's body for evidence" as implicating "expectations of privacy and security of such magnitude that the intrusion may be 'unreasonable' even if likely to produce evidence of a crime." *See* Winston v. Lee, 470 U.S. 753, 759 (1985) (holding that the Fourth Amendment prohibited the state from surgically extracting a bullet from a criminal suspect in order to collect evidence).

94. *Birchfield*, 136 S. Ct. at 2184.

95. In his *Jones* concurrence, Justice Alito anticipated that a trespass test "will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked." United States v. Jones, 565 U.S. 400, 426 (2012) (Alito, J., concurring) (offering the example of police surreptitiously activing a car's stolen vehicle detection system). Moreover, in 2016, the

intrusion experienced by the offender would be rather minimal. From this basic framework, we can then add nuance. For example, haptic feedback technologies that use vibration or other forms of physical or auditory force to notify an offender of potential violations would likely add to the experienced intrusiveness, even if the device was otherwise physically unimposing,[96] in the same way we can imagine a breathalyzer that is designed in a way to be painful or strange to use.

Currently available monitoring technology sits somewhere in the middle of this continuum. First-hand accounts from Michigan sex offenders subject to lifetime monitoring reveal the substantial physical burden technological monitoring devices *can* impose. The device used for lifetime monitoring in Michigan at the time was even larger than a traditional GPS ankle monitor.[97] The weight of the device could rub the underlying skin raw or cut into the skin and cause bleeding.[98] The device is designed to vibrate for particular alerts, and can also cause electric shocks when it malfunctions.[99] Technological monitoring can also be physically incapacitating: the technology used in Michigan required the offender to remain plugged into a wall outlet for at least two hours each day to allow the device to charge.[100] Charging cannot realistically be performed while sleeping because movement will disconnect the charger, triggering a vibration that further disrupts sleep.[101] Individuals subjected to devices of this sort appear to view them as similar to a classic ball and chain, which might have weighed only 18 pounds,[102] and yet was

---

Tenth Circuit Court of Appeals published a decision in which (then Circuit Judge, now Supreme Court Justice) Neil Gorsuch held that the government conducted a trespassory *Jones* search without a physical invasion when it opened the defendant's emails via a remote web browser. *See* United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).

96. Amazon recently made headlines when it patented worker monitoring wristbands that could alert a worker to possible mistakes or deviations in a similar manner. *See* Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)*, N.Y. TIMES (Feb. 1, 2008), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

97. Brief for the ACLU of Mich. and the Crim. Def. Atty's of Mich. as Amici Curiae, People v. Cole, 817 N.W.2d 497(Mich. 2012) (No. 143046), 2012 WL 697464, at *App'x.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. *Found: The Ball and Chain That May Have Condemned a 17th Century Prisoner to a Watery Grave in the Thames*, DAILY MAIL (Aug. 27, 2009, 10:28 AM), http://www

nevertheless exasperating (and historically and socially salient) precisely because its wearer could never be free of it.[103] There was no lull in the intrusion.

Against this backdrop, Judge Posner's casual equating of offender monitoring technology with the GPS devices used to track "hikers," "kids," or "elderly relatives" is inaccurate and seems disingenuous.[104] As *Birchfield* demonstrates, one measure of the intrusiveness of a given technology is the availability of a less invasive alternative.[105] Yet thus far the devices used to track sex offenders are substantially more onerous than consumer versions of GPS technology.[106] Consider that in the span of just a few years, GPS monitoring technologies have not only advanced in technological sophistication, but have been dramatically reduced in their physical dimensions.[107] A modern-day GPS chip is approximately the size of a postage stamp; a similar device from a decade earlier would have been more comparable to a thick stack of index cards.[108] In addition to being smaller and lighter, current monitoring devices are often styled in ways that mimic traditional fashion accessories—such as bracelets and wristwatches—and are therefore simply less "strange" than the sizable ankle devices often used for offenders, which are echoes of historical prisoner restraints, such as shackles and leg irons.[109]

.dailymail.co.uk/news/article-1209405/First-intact-ball-chain-drowned-prisoner-mud-Thames.html.

103. *Cf.* Wayne A. Logan, *Federal Habeas in the Information Age*, 85 MINN. L. REV. 147, 194–99 (2000) (discussing various ways in which burdens imposed by sex offender registration and community notification laws result in a "hidden" custody sufficient to warrant federal habeas corpus protection).

104. *See* Belleau v. Wall, 811 F.3d 929, 931 (7th Cir. 2016).

105. Birchfield v. North Dakota, 136 S. Ct. 2160, 2178, 2184 (2016).

106. Some monitoring regimes require released sex offenders to pay for their own monitors. *See* MICH. COMP. LAWS ANN. § 791.285(2) (West 2006); *Lifetime Electronic Monitoring Program—Current Daily Rate*, MICH. DEP'T. OF CORRECTIONS (Oct. 1, 2014), http://www.michigan.gov/documents/corrections/Current_Daily_Rate_for_Lifetime_Electronic_Monitoring_Program_353451_7.pdf. Although the practice of making criminal offenders pay for their punishment is not uncommon, *see* Cook, *supra* note 3, having released sex offenders pay for the government to search them may be relevant to the extent of the Fourth Amendment intrusion.

107. *See* Jordan Miller, *New Age Tracking Technologies in the Post*-United States v. Jones *Environment: The Need for Model Legislation*, 48 CREIGHTON L. REV. 553, 560–65 (2015).

108. *See id.* at 563–64.

109. Although shackles and leg irons are not "strange" in at least one sense—they have a long history of use—the *Birchfield* Court's reference to "painful or strange" physical

This comparison suggests a lasting significance for *Jones* in non-investigative contexts. Some commentators have questioned the utility of a Fourth Amendment trespass test, given that the need of law enforcement to reduce inconvenience and the risk of detection provides a strong incentive for the government to continue developing and using less physically intrusive monitoring technologies.[110] Indeed, the pervasive use of consumer technology that performs similar types of monitoring—from cellular phones to vehicle navigation systems to personal fitness trackers—may provide the government with avenues for surveillance that render physical intrusion entirely unnecessary.[111] For these reasons, we might correctly anticipate that the number of successful *Jones* challenges to investigative searches will be both small and decreasing in the face of technological advancements. However, the same logic suggests that *Jones* may ultimately have a lasting and substantial role to play in the post-release monitoring context, in which the government lacks the same inherent incentives—primarily, fear of detection and evasion—to develop and employ less physically intrusive technologies. In fact, in these situations, individual government actors may have colorable reasons for imposing a greater level of physical intrusion than necessary—a cost borne solely by the citizen being monitored—in service of seemingly sensible goals, such as the financial savings (or simply the ease) of delaying upgrades to outdated technology.[112] A Fourth Amendment jurisprudence that bars unreasonable physical intrusions, forcing the government to be thoughtful and careful in how it buys and deploys monitoring technology, can change the landscape.

B. Too Much Information: A "Mosaic" Theory of Intrusion

In addition to intruding on individuals physically, the technological monitoring of convicted sex offenders intrudes on those individuals' privacy

---

intrusions operates by comparing the challenged intrusion to the everyday activities of ordinary citizens. A breath test is minimally intrusive when it is analogous to drinking out of a straw. *Birchfield*, 136 S. Ct. at 2177. A blood test is significantly more intrusive when it is analogous to a blood draw during an annual physical exam, a process that few relish and some try to avoid. *Id.* at 2178. Shackles and leg irons lack a clear analog in everyday life, and are therefore an indisputably "strange" form of physical intrusion for most citizens.

110. Miller, *supra* note 107, at 563.

111. *See* United States v. Jones, 565 U.S. 400, 414–15 (2012) (Sotomayor, J., concurring).

112. Moreover, government actors may view themselves as having an affirmative incentive to increase the physical burden of a monitoring technology as a punitive measure.

because it collects large quantities of information. Although Justice Scalia's majority opinion in *Jones* emphasized the physical trespass involved, five members of the *Jones* Court also expressed concerns that extended monitoring would amount to a Fourth Amendment search even under the *Katz* test. Justice Sotomayor joined Scalia's majority opinion, relying on trespass, but also wrote separately to offer her view that technological advances may uniquely threaten citizen privacy by allowing a depth of surveillance not previously possible at a fraction of the cost of traditional methods.[113] She expressed not only doubt that "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," but also unease at the government's wielding "a tool so amenable to misuse."[114] Justice Alito's concurrence, joined by three other Justices, likewise emphasized the intrusiveness of extended technological surveillance.[115] Calling the four-week continuous tracking of the suspect's vehicle "lengthy," Alito reasoned that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[116]

At the core of these Justices' concerns is what has come to be known as the "mosaic theory" of Fourth Amendment privacy—"the idea that certain types of governmental investigation enable accumulation of so many individual bits about a person's life that the resulting personality picture is worthy of constitutional protection."[117] Here is how the D.C. Circuit first

113. *See Jones*, 565 U.S. at 415–16 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

114. *Jones*, 565 U.S. at 416.

115. *See id.* at 418–19 (Alito, J. concurring). Justices Ginsburg, Breyer, and Kagan joined Alito's concurrence.

116. *Id.* at 430.

117. Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of the Mosaic Theory*, 8 DUKE J. CON. L. & PUB. POL'Y 1, 3–4 (2012).

articulated the mosaic theory in *United States v. Maynard*, which became *Jones* before the Supreme Court:

> [The] whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.[118]

Scholars and commentators have addressed at length the utility and practicability of adopting the mosaic theory.[119] We do not intend to revisit that ground. Rather, we are particularly interested in considering what weight, if any, concerns about the intrusiveness of data aggregation have in analyzing whether a search is constitutionally unreasonable. The mosaic theory is traditionally thought to be mostly relevant to the predicate question whether a Fourth Amendment search has occurred.[120] However, the particular concerns about the intrusiveness of monitoring that drive the mosaic theory in the first instance also seem apropos to resolving the further question whether a specific search was constitutionally reasonable.

Consider again Justice Sotomayor's concurrence in *Jones*. She identified several "unique attributes of GPS surveillance" that require careful attention.[121] First, the monitoring is "precise" and "comprehensive."[122] Second, the government can store the records generated by monitoring technologies "and efficiently mine them for information years into the future."[123]

---

118. *Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

119. For a thorough overview of the origins of the mosaic theory, see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

120. *See id.* at 312–13. As noted above, the *Jones* Court did not evaluate the reasonableness of extended technological monitoring, despite five members of the Court endorsing something akin to the mosaic theory. *Jones*, 565 U.S. at 413 ("We consider the argument [that the search was reasonable] forfeited."). *See also id.* at 416–17 (Sotomayor, J., concurring) (noting that the intrusiveness of GPS monitoring is relevant to "the existence of a reasonable societal expectation of privacy in the sum of one's public movements," but declining to resolve that question); *id.* at 430–31 (Alito, J., concurring) (explaining that "the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment" without analyzing whether the search was reasonable).

121. *Id.* at 415 (Sotomayor, J., concurring).

122. *Id.*

123. *Id.* Notably, the Supreme Court quietly expressed a similar concern about the storage and future use of collected data in *Birchfield*, the breathalyzer and blood test case

Taken together, she fears that these two features result in monitoring that "chills associational and expressive freedoms."[124] Third, the technology is (relatively) inexpensive, allowing the government to conduct searches unconstrained by the resource limitations that might have previously curtailed abusive practices.[125] All three concerns quite clearly extend to the technological monitoring of convicted sex offenders. The first two of Sotomayor's concerns echo the work of legal scholars who claim that excessive surveillance can have a crippling effect on individuals.[126] For example, Jed Rubenfeld has argued that the Fourth Amendment principally exists to protect an individual's personal life, which he conceptualizes as a space "where people are supposed to be free from the strictures of public norms, free to be their own men and women, free to say what they actually think, and to act on their actual desires or principles, even if doing so defies public norms."[127] The third concern reflects the longstanding fear that widespread surveillance will be destructive of the relationship between citizens and the government.[128] Although this idea has never been given a special doctrinal formulation, courts and commentators have long posited that the Fourth Amendment serves as a check against "a too permeating police surveillance."[129]

Wisconsin's technological monitoring program, at issue in *Belleau*, entailed several programmatic decisions that arguably mitigate the set

---

from the same Term as *Jones*. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016) (noting that blood samples can be preserved for some length of time and can reveal information beyond blood-alcohol content, thus generating anxiety about unanticipated future uses for those subjected to a blood draw). *See generally* Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1, 3 (2018).

124. *Jones*, 565 U.S. at 416.

125. *Id.* at 415–16.

126. *See* Sklansky, *supra* note 85, at 1095–97 (surveying the scholarship arguing for what he terms the "stultification thesis"—"the belief that surveillance deters the kinds of activities and communications necessary for people to lead full lives as individuals and democratic citizens"). *See generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH 202–03 (Alan Sheridan trans., 2d ed. 1995) ("He who is subjected to a field of visibility, who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relations in which he simultaneously plays both roles; he becomes the principle of his own subjection.").

127. Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 128 (2008).

128. *See generally* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1104–07 (2002) (articulating the dangers of governmental information gathering).

129. United States v. Di Re, 332 U.S. 581, 595 (1948).

of concerns addressed by the mosaic theory. With respect to the concern over increased *police* surveillance power due to reduced surveillance costs, Judge Flaum in a concurring opinion explained that Wisconsin's monitoring program had, as a matter of course, relatively little police involvement:

> Police do not administer the program, or even access the GPS data unless they have some reason to specifically request it. Even the Department of Corrections does not review Belleau's location in real-time, but only at the end of each day. Additionally, the program is narrowly designed only to track Belleau's location.[130]

The use of third parties (including private parties) to perform governmental tracking is actually quite common.[131] An important question, however, is whether the use of third parties has privacy benefits that might minimize the intrusiveness of a government search. On the one hand, the raging debate over the much-maligned third-party doctrine demonstrates that people are particularly uncomfortable providing the government with access to information that they freely, if often unknowingly, provide to private companies.[132] On the other hand, and perhaps relatedly, the dangers of surveillance are increasingly understood to be a function of the interaction of both public- and private-sector information collection.[133] Although the Wisconsin program ultimately put sex offender monitoring data in the hands of its Department of Corrections in the first instance, rather than its police, it does not erect any barriers to police accessing that data, other than the effort of making the request. Moreover, by disseminating the information to a larger number of parties, greater exposure occurs—to more people in more roles. For the same reason, a monitoring program such as Wisconsin's increases the risk of data leakage and various other privacy harms—including blackmail, coercion, and discrimination.[134]

A more promising feature of the Wisconsin program, at least from a privacy perspective, is the lack of active monitoring. Judge Posner

---

130. Belleau v. Wall, 811 F.3d 929, 941 (7th Cir. 2016) (Flaum, J., concurring).

131. *See, e.g.,* Commonwealth v. Feliz, No. 16-00077, 2017 WL 1450461, at *2 (Mass. Super. Apr. 21, 2017) (describing Massachusetts's partnership with 3M).

132. *See* Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?* 74 FORDHAM L. REV. 1731, 1745 (2006).

133. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1958 (2013).

134. *Id.* at 1952–58.

emphasized this fact in his *Belleau* opinion, juxtaposing problematic governmental surveillance techniques—"following the plaintiff around . . . trailing him as he walks to the drug store or the local Starbucks"—with the nightly mapping conducted by the Wisconsin Department of Corrections:

> [E]very night the Department of Corrections makes a map of every anklet wearer's whereabouts that day so that should he be present at a place where a sex crime has been committed, or be hanging around school playgrounds or otherwise showing an abnormal interest in children not his own, the police will be alerted to the need to conduct an investigation.[135]

In his concurrence, Judge Flaum described this as a lack of "real-time" monitoring, a characterization sometimes used by courts.[136] But we think that few of the privacy implications of active versus passive monitoring turn solely on *when* the monitoring is conducted.[137] Rather, the crux of the concern about real-time monitoring appears to be that it draws the government's attention to large quantities of information that are irrelevant to the ultimate aim of deterring future crime. As Posner alluded to in his opinion, real-time, active monitoring requires that equal attention is paid to a convicted sex offender's trip to Starbucks and his trip to a local school or playground.[138] Passive monitoring technologies, which alert law enforcement only when the information collected suggests a problem (potentially after some processing delay, as in Wisconsin's daily mapping regime), are

---

135. *Belleau*, 811 F.3d at 935.

136. A handful of courts have intimated that the constitutionality of cell phone location tracking may depend on whether the information collected is "historical" rather than "real time." *See, e.g.*, Tracey v. State, 152 So. 3d 504, 512–19 (Fla. 2014) (surveying federal law). *But see* Orin Kerr, "Florida Supreme Court Holds Real-Time Cell-Site Data Protected under Fourth Amendment," VOLOKH CONSPIRACY (Oct. 16, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/10/16/florida-supreme-court-holds-real-time-cell-site-data-protected-under-fourth-amendment ("That distinction matters in the statutory context because the Stored Communications Act expressly regulates historical access but does not regulate real-time access. But I don't see how it could matter for purposes of the Fourth Amendment question of what is a 'search.'").

137. The idea of persistent, real-time observation may feel inherently intrusive in the abstract. But one can easily construct hypotheticals involving transmission delays of seconds, minutes, or even hours that quickly undermine the instinct that timing, as opposed to the nature and quantity of information collected, is the source of the intrusion.

138. *Belleau*, 811 F.3d at 935.

thus less intrusive in the sense that they are able to distinguish relevant from irrelevant information.[139]

Being able to distinguish relevant from irrelevant information speaks directly to Justice Sotomayor's first two concerns—the propensity of comprehensive surveillance to produce chilling effects on associational and expressive freedoms.[140] Knowing that the government is watching may dissuade monitored offenders from acting on their authentic preferences, even with respect to activities that have nothing to do with the likelihood of recidivism. Traditionally, the Fourth Amendment has protected against "dragnet" searches and "fishing expeditions" by requiring particularized suspicion of criminal wrongdoing as a predicate to a search.[141] "Particularized suspicion keeps the government's profound investigative powers in check preventing widespread surveillance and snooping into the lives and affairs of all citizens."[142] In the context of sex offender monitoring, passive monitoring technologies may function as a surrogate for a suspicion requirement, and thus better comport with the animating principles of the Fourth Amendment, either by reducing the salience of irrelevant information or by keeping it from the authorities altogether.[143]

---

139. Real-time monitoring by a human does dangle the possibility of additional law enforcement benefits, however: the intervention and prevention or disruption of a crime as it is about to occur or is occurring (perhaps in an unexpected way that any passive monitoring technology is less likely to detect). Passive monitoring as deployed seems to build in a delay in law enforcement responsiveness and necessarily operates on the basis of backward-looking offender behavioral patterns. As technology improves, alert systems relying on advanced prediction technology may reduce or eliminate or even reverse any advantage of a human being monitoring a sex offender in real time.

140. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

141. *See* Solove, *supra* note 128, at 1107. One of the paradigmatic evils that the Fourth Amendment was enacted to restrain is the "indiscriminate rummaging" permitted by general warrants. *See* Walter v. United States, 447 U.S. 649, 656 (1980) (plurality opinion).

142. Solove, *supra* note 128, at 1109. Scholars concerned about the growing state of governmental surveillance frequently tout similar benefits from Title I of the Electronic Communications Privacy Act of 1986 (ECPA). *See* Richards, *supra* note 133, at 1962. The ECPA requires that warrants for wiretaps be for a limited time and that the wiretapping be "conducted in such a way as to minimize the interception of information not relevant to the warrant." *Id. See generally* 18 U.S.C. §§ 2510–22.

143. We note, however, that passive monitoring programs typically involve the storage of monitoring data for some period of time. The preservation of such data raises the specter of future mining and use by the government, which may be of constitutional significance. *See supra* note 123.

On this score, Wisconsin's daily mapping regimen likely occupies a middle ground in its intrusiveness. All of the locations of a monitored individual in a given day are ultimately observed by the Department of Corrections. But the aggregation of an entire day's worth of movements may minimize the attention paid to any particular movement, particularly if the government is sincere in its assertion that the daily maps are used only to evaluate whether the offender engaged in any conduct that warrants further investigation by the police.[144] Other, even less intrusive programs are certainly possible. Massachusetts, for example, collects and preserves location data, but does not typically review the data unless an automated alert has been triggered by an event such as a monitored individual entering an exclusion zone.[145]

C. "Intimacy" and Intrusion: Preserving Privacy at Home

While the informational privacy analysis set forth above emphasizes the quantity of information the government collects, and who (and how often they) can view it, the Fourth Amendment also imposes strict limitations on the kind of information that may be collected through the technological monitoring of convicted sex offenders. The Fourth Amendment has long afforded special protection to information and locations associated with traditionally "intimate" behavior, the home chief among them.[146] Houses are expressly included in the text of the Fourth Amendment as an

144. Judge Posner suggested a rather tenuous distinction between a device that "just identifies locations" and one with the capability to "reveal what the wearer of the device is doing at any of the locations." *See* Belleau v. Wall, 811 F.3d 929, 936 (7th Cir. 2016). Obviously, one's conduct can be inferred with some level of accuracy from one's movements, even if such inferences are at times off the mark. We are more persuaded that Department of Corrections employees will be disinclined to spend the time and mental effort necessary to draw such inferences in the first place when they are tasked with mapping aggregated information in search of specific, suspicious movements.

145. *See* Commonwealth v. Feliz, No. 16-00077, 2017 WL 1450461, at *2 (Mass. Super. Apr. 21, 2017).

146. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 179 (1984) ("[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference . . . ."); United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972) ("[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed . . . .").

embodiment of the centuries-old respect afforded the sanctity and privacy of the home.[147] At times, the Supreme Court has implied that the Fourth Amendment draws a clear line at the entrance to the home, including in one of the earliest cases on technological monitoring.[148] The Court has also suggested more often of late that the constitutional protection of the home serves to prophylactically protect the personal intimacies that typically take place within that sphere.[149]

Perhaps the clearest illustration of the Fourth Amendment's protection of the intimacies of the home can be seen in *Kyllo v. United States*.[150] There, the Supreme Court confronted the government's use of technology to detect heat signatures emanating from the exterior of a home.[151] Tellingly, Justice Scalia's majority opinion framed the constitutional inquiry as "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[152] The Court expressed skepticism about the government's use of "a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion."[153] Although the technology in question was deployed to confirm the suspected cultivation of marijuana, the *Kyllo* Court feared it might equally be used to "disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath."[154] Despite offering this particularly evocative (if problematic)[155] depiction of an "intimacy" that

147. *See, e.g.*, Payton v. New York, 445 U.S. 573, 590, 591–98 (1980) (proclaiming that "the Fourth Amendment has drawn a firm line at the entrance to the house" and surveying English common law regarding warrantless entries into the home).

148. *E.g. id.*; United States v. Karo, 468 U.S. 705, 714–18 (1984) (holding that a warrant was required to monitor the signal of an electronic beeper once it entered a private home).

149. During oral argument in *Carpenter v. United* States, a case that will decide the Fourth Amendment status of cell phone location data, Justice Sotomayor drew laughs with her insight that the location data is emanating from a device that many now use on the toilet and carry with them to bed. *See* Carpenter v. United States, No. 16-402, transcript pp. 42–43 (Nov. 29, 2017), *available at* https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf.

150. *Kyllo*, 533 U.S. 27 (2001).

151. *Id.* at 29.

152. *Id.* at 34.

153. *Id.*

154. *Id.* at 38.

155. *See* Jeannie Suk, *Is Privacy a Woman?*, 97 GEO. L. J. 485, 488–89 (2009) (highlighting the "anachronism" of this imagery, which posits privacy as "a woman, the object of the male gaze."). *See generally* CATHARINE A. MACKINNON, *Privacy v. Equality: Beyond* Roe v. Wade,

the Fourth Amendment shields from exposure, the Court explained that the outcome does not depend on the specific information actually revealed by the search: "In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."[156] *Kyllo* is thus paradigmatic of a broad trend in Fourth Amendment jurisprudence to protect from governmental intrusion the stereotypical American home.

One helpful approach to thinking about the Fourth Amendment's traditional privileging of the home has been offered by Kerr's "equilibrium-adjustment theory" of the Fourth Amendment, which contends that judges respond to new technologies and social practices by adjusting the Fourth Amendment's protections so as to restore a historical balance between the needs of law enforcement and individual liberty.[157] "When new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[158] Whether or not the judicial responses that Kerr identifies are intentional efforts to restore a balance, an equilibrium-adjustment theory of the Fourth Amendment has considerable explanatory power. The Supreme Court, in particular, has frequently analogized modern-day governmental searches to historical Anglo-American legal practices in order to evaluate their permissibility.

On an equilibrium-adjustment theory, we should expect that technological monitoring of sex offenders would be on its most tenuous constitutional footing when it captures information within the home. As far back as the dawn of the seventeenth century, an English court famously observed that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose."[159] William Blackstone reiterated that sentiment in his *Commentaries on the*

---

in FEMINISM UNMODIFIED: DISCOURSES ON LIFE & LAW 101 (1983) ("From this perspective, the legal concept of privacy can and has shielded the place of battery, marital rape, and women's exploited labor; has preserved the central institutions whereby women are *deprived* of identity, autonomy, control and self-definition; and has protected the primary activity through which male supremacy is expressed and enforced.").

156. *Kyllo*, 533 U.S. at 37.

157. *See* Kerr, *supra* note 41, at 517–18.

158. *Id.* at 480.

159. Semayne's Case, 77 Eng. Rep. 194, 195 (K.B. 1603). For a brief critique of the wisdom of extending the historical castle metaphor to contemporary legal systems, see Ben A. McJunkin, *Rank Among Equals*, 113 MICH. L. REV. 855, 870 (2015).

Laws of England, noting that "the law of England has so particular and tender a regard to the immunity of a man's house, that it stiles it his castle, and will never suffer it to be violated with impunity. . . . For this reason no doors can in general be broken open to execute any civil process; though, in criminal causes, the public safety supersedes the private."[160] Politicians, courts, and commentators ensured that this principle became part of the fabric of early American law. As Thomas Cooley observed in his famous 1868 constitutional law treatise, "it is better oftentimes that crime should go unpunished than that the citizen should be liable to have his premises invaded, his trunks broken open, his private books, papers, and letters exposed to prying curiosity, and to the misconstructions of ignorant and suspicious persons."[161] And, indeed, the Supreme Court has routinely struck down the government's use of modern technology to collect information about the interior of a citizen's home.[162]

The technological monitoring of sex offenders thus poses a unique Fourth Amendment dilemma. One would expect that a careful Fourth Amendment analysis of technological monitoring would recognize that the nature of information collected informs whether a search is reasonable by taking into account whether the information in question is especially intimate *and* whether it has any realistic connection to monitoring's legitimate goals (i.e., recidivism reduction). Modern GPS technology has the ability to pinpoint a user's location to within about three meters (roughly ten feet).[163] That level of accuracy is useful for effectively monitoring individuals' movements outside of the home. Yet it is also quite possibly sufficient to locate an individual *within* a specific room of a home. It is easy to imagine that future monitoring technologies will be able to generate location information that is even more precise and perhaps makes available other details as well, such as a person's directional orientation, whether the person is standing or sitting or lying down (i.e., using altitude measurements and gyroscope technology), etc. We may soon reach a point where the government has the power not only to identify when the (monitored)

160. William Blackstone, 4 Commentaries 223 (1765–1769).

161. Thomas M. Cooley, A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union 306 (1868).

162. *E.g.*, *Kyllo*, 533 U.S. at 37; *Karo*, 468 U.S. at 714–18.

163. Tim Kolesk, Note, *At the Intersection of Fourth and Sixth: GPS Evidence and the Constitutional Rights of Criminal Defendants*, 90 S. Cal. L. Rev. 1299, 1302 (2017).

lady of the house takes her daily bath, but also to distinguish a trip to the bath from a trip to the toilet. This would be an unprecedented level of intrusion for the Fourth Amendment to countenance without a warrant or an exception to it.

In addition, the nature of technological monitoring seems very likely to continue to evolve beyond simple geolocation and physical orientation tracking. Although monitoring devices that generate audio or video recordings within the home would likely be considered so invasive as to be presumptively unreasonable, currently available consumer technology hints at other avenues of possible intrusion into traditionally protected intimacies.[164] Imagine, for example, a technological monitoring program that outfitted convicted sex offenders with heartrate or blood pressure monitors to detect patterns that might indicate heightened sexual arousal (and hence a potential opportunity for recidivism). We might view such an intrusion as beyond the pale, even where the information gained by monitoring has some meaningful benefit to the government's aims.[165] Intrusions in this category are almost instinctively offputting, and may be less amenable to trade-offs than those in other categories.

These observations suggest that the government's use of monitoring technology may need to be tailored to preserve the sanctity of intimate information within the home. Fortunately, there is no obvious reason why technology that has additional monitoring capacity cannot also be fitted with checks to allow extreme monitoring only when particularly justified, with protections against intrusions in place whenever an individual is at home. As it continues to develop, monitoring technology will become better able to collect much *more* information, allowing greater depth and focus, but also will become better able to algorithmically "unfocus" when the information to hand is intimate or irrelevant. But, importantly, technology producers may require encouragement by courts or legislatures to develop ways to limit the reach of their own products, since those who buy and deploy monitoring technology are unlikely to worry too much about

164. One concern here is that courts may prove less willing to give normative privilege to the intimacies of sex offenders who have demonstrated their divergence from accepted social norms.

165. Indeed, the level of intrusion seems to magnify if we imagine future technologies that allow the monitoring to be more precise—e.g., monitoring for specific muscle contractions, blood flow to specific body parts, or pupil dilation.

overinclusive data collection—after all, extra, unnecessary data can always be ignored—absent some pressure from government actors.

D. Search as Spectacle: Dignitary Harms and the Fourth Amendment

A fourth, and final, dimension of intrusion relates to the visibility of technological monitoring. To individuals being monitored, the *visibility* of the technology to the public is one of the most tangible and salient burdens that a governmental monitoring regime imposes. Wearable technology—such as a traditional ankle monitor—immediately brands the wearer as a criminal or other undesirable, inviting stigma, ostracism, and even confrontation.[166] Fourth Amendment search jurisprudence, however, has historically had little to say about social stigma. Judges frequently dispatch such arguments summarily, as if they are minor grievances of no doctrinal significance.[167] Meanwhile, scholarly consideration of the spectacle of search remains rare, often classified as an outsider critique.[168] Nevertheless, we view search stigma as a critical consideration because many of the values that the Fourth Amendment aims to protect are threatened or impinged by search practices that publicize past criminality and ongoing suspicion.

Consider, for example, the disfavored constitutional status of "media ride-alongs." Early one morning in 1992, a team of U.S. Marshalls and Maryland police officers attempted to execute arrest warrants for a known fugitive by entering the residence listed as his address.[169] Because the excursion was part of a special national fugitive apprehension program—dubbed "Operation Gunsmoke"—the marshals had invited a reporter and photographer from the *Washington Post* to accompany them.[170] Unknown to the government agents involved, however, they had actually entered the

166. *See, e.g.*, Brief of Plaintiff-Appellee at *6, Belleau v. Wall, 811 F.3d 929 (7th Cir. 2016) (No. 15-3225) (recounting that "[a] neighbor who learned Belleau was a sex offender brandished a gun and warned him to stay away, and others stopped speaking with him").

167. Consider Judge Posner's minimizing description of the plaintiff's burden in *Belleau*: "When the ankleted person is wearing trousers the anklet is visible only if he sits down and his trousers hike up several inches and as a result no longer cover it." *Belleau*, 811 F.3d at 932.

168. *See, e.g.*, I. Bennett Capers, *Policing, Race, and Place*, 44 HARV. C.R.-C.L. L. REV. 43, 68–69 (2009).

169. Wilson v. Layne, 526 U.S. 603, 606–07 (1999).

170. *Id.*

home of the fugitive's parents, Charles and Geraldine Wilson.[171] The *Post*'s photographer captured the chaos that ensued. Believing him to be their target, officers quickly subdued an angry, cursing Charles Wilson, dressed only in a pair of briefs.[172] Geraldine Wilson, dressed in a thin nightgown, looked on.[173] Eventually, the government agents learned that their true target was not in the home, and they departed; the photographs of the incident were never published.[174] The Wilsons, however, brought a Section 1983 action seeking monetary damages for being subjected to an unreasonable search.[175]

The Wilsons' lawsuit reached the Supreme Court in the fall of 1998. Chief Justice Rehnquist authored the Court's opinion, which began by conceding that the government agents "were undoubtedly entitled to enter the Wilson home in order to execute the arrest warrant."[176] "But it does not necessarily follow that they were entitled to bring a newspaper reporter and a photographer with them," Rehnquist added.[177] Doctrinally, the issue before the Court was whether the media's presence was so unrelated to the purpose of the search as to render an otherwise lawful entry into the home unreasonable.[178] And, in fact, the government had identified several legitimate law enforcement goals that were arguably furthered by the media ride-along, including the possibility that the presence of reporters might protect suspects and minimize police abuses, much in the same way that police dash cams and body cams are now justified.[179] The Court was unanimously unpersuaded.[180] Justice Rehnquist (and the rest of the *Wilson* Court) drew a clear distinction between reasonable "quality control" measures, including potentially police-operated cameras, and the presence of "Washington Post reporters in the Wilsons' home . . . working on a story for their own purposes."[181] This distinction hints at something deeper than

171. *Id.* at 606.
172. *Id.* at 607.
173. *Id.*
174. *Id.* at 607–08.
175. *Id.* at 608.
176. *Id.* at 611.
177. *Id.*
178. *Id.*
179. *See id.* at 611–13.
180. Justice Stevens concurred that the Fourth Amendment was violated, but dissented on the separate question whether the officers were entitled to qualified immunity.
181. *Id.* at 613.

simply the *purposelessness* of a third party's presence during a police search: It was that *the purpose was to publicize*. It was the specter of spectacle that was so troubling to the Court. Despite the fact that the Post had published neither a story of the search nor any of the photographs taken, Rehnquist's opinion repeatedly framed the analysis in a way that emphasized the unseemliness of bringing "the media" into a "private home."[182]

Wilson represents but one example of how the Fourth Amendment constrains the methods police may use to accomplish their objectives. In particular, the case suggests that publicity of criminality may itself be a cognizable form of privacy invasion. It is far from alone in that respect. The Supreme Court has at times weighed the "public stigma associated with the search" in assessing the reasonableness of police conduct.[183] It has intimated that searches may be especially intrusive when they connote criminality, serving as a "badge of shame."[184] Lower federal courts have repeatedly considered whether an otherwise lawful search or seizure was rendered unreasonable by subjecting a suspect to the "stigma" and "indignity" of remaining unclothed for a prolonged period.[185] Scholars have taken these privacy-based concerns about publicizing criminality even further. Bill Stuntz once wrote about the "invasions of dignitary interests" that accompany many constitutional policing practices when they occur in public: "Arrests or street stops infringe privacy in this sense because they stigmatize the individual, single him out, and deprive him of freedom."[186]

---

182. *See id.* at 605, 608, 613–15.

183. *See, e.g.,* Michigan v. Summers, 452 U.S. 692, 702 (1981) (reasoning that detention of a person in a private residence "would involve neither the inconvenience nor the indignity associated with a compelled visit to the police station").

184. Veronia Sch. Dist. 47 v. Acton, 515 U.S. 646, 663 (1995).

185. *See, e.g.,* Hutchinson v. W. Va. State Police, 731 F. Supp. 2d 521, 537 (S.D. W.Va 2010); Bancroft v. City of Mount Vernon, 672 F. Supp. 2d 391 (S.D.N.Y. 2009); Luster v. Ledbetter, 647 F. Supp. 2d 1303 (M.D. Ala. 2009). In fact, there appears to be substantial overlap between the language courts employ in describing the harms of publicity and the language they employ in describing the invasiveness of strip searches generally. *See* Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 374–75 (2009) (describing the "indignity" of a "degrading" strip search of a student, who recounted the experience as "embarrassing, frightening, and humiliating"). Although strip searches do not take place in public, the reason that courts treat strip searches as categorically distinct is precisely because of this concern for the stigma and indignity of being "seen" by "others" in a particular way.

186. William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1021 (1995).

More recently, numerous scholars have demonstrated the slew of ways that the public stigma associated with subjection to basic policing tactics, such as the classic *Terry* stop, reinforce harmful social models of race and gender.[187] Similar arguments have been marshalled to support Fourth Amendment challenges to the stigmatizing practices ranging from drug-dog sniffs[188] to "perp walks."[189]

Much like a perp walk, or a mug shot,[190] the traditional ankle monitor is an archetypal display of criminality. It is sufficiently entwined into the American cultural consciousness, being regularly referenced in popular culture and satirized in social media, as to be easily recognized by most members of the public.[191] Because of the cultural meaning attached, an ankle monitor's presence is also expressive—its presence communicates something about both the deviance and dangerousness of the person wearing it.[192] In contexts outside of the Fourth Amendment, the spectacle of sex offender monitoring has found resonance with some courts.[193] In finding that monitoring was an unconstitutional punishment, the Supreme Court of New Jersey recently opined on its stigmatizing effects:

---

187. *See, e.g.*, Paul Butler, *Stop and Frisk and Torture-Lite: Police Terror of Minority Communities*, 12 OHIO ST. J. CRIM. L. 57 (2014); Frank Rudy Cooper, *"Who's the Man?": Masculinities Studies,* Terry *Stops, and Police Training*, 18 COLUM. J. GENDER & L. 671 (2009); Kaaryn Gustafson, *Degradation Ceremonies and the Criminalization of Low-Income Women*, 3 U.C. IRVINE L. REV. 297, 304–36 (2013).

188. Jordan Blair Woods, *Decriminalization, Police Authority, and Routine Traffic Stops*, 62 UCLA L. REV. 672, 723–24 (2015) ("When police use drug-sniffing dogs during a non-criminal traffic stop, they communicate the message that the motorist is not simply a non-criminal traffic violator, but also a potential drug criminal. These messages can have humiliating and stigmatizing effects on innocent civilians, especially racial minority motorists more commonly subjected to drug-sniffs during pretextual traffic stops.").

189. Palma Paciocco, *Pilloried in the Press: Rethinking the Constitutional Status of the American Perp Walk*, 16 NEW CRIM. L. REV. 50, 101 (2013). ("The perp walk does violence to a person's dignity and privacy. It is a highly public, highly ritualistic event that stigmatizes and humiliates.").

190. *See id.* (discussing JONATHAN FINN, CAPTURING THE CRIMINAL IMAGE: FROM MUG SHOT TO SURVEILLANCE SOCIETY viii (2009)).

191. Although the monitored offender has some ability to avoid the stigma of publicity, those efforts may require substantial changes to one's life, a cost that is too easily overlooked or minimized in the legal analysis of intrusion. *See supra* note 167.

192. Eisenberg, *supra* note 1, at 141.

193. Commonwealth v. Cory, 911 N.E.2d 187, 196 (Mass. 2009) ("As 'continuing, intrusive, and humiliating' as a yearly registration requirement might be, a requirement permanently to attach a GPS device seems dramatically more intrusive and burdensome.").

> Even though [the statute's] purpose is not to shame Riley, the "effects" of the scheme will have that result. If Riley were to wear shorts in a mall or a bathing suit on the beach, or change clothes in a public locker or dressing room, or pass through an airport, the presence of the device would become apparent to members of the public. The tracking device attached to Riley's ankle identifies Riley as a sex offender no less clearly than if he wore a scarlet letter.[194]

In sum, technological monitoring of sex offenders has the potential to work a particular kind of dignitary and privacy harm, one that is increasingly cognizable in constitutional analysis generally.[195] Unlike the intrusions discussed in prior sections, this harm emanates not from the quantity or quality of private information collected in the government's search, but rather from the very spectacle of the search itself.

Fortunately, the stigmatizing potential of sex offender monitoring regimes is almost entirely a function of the technology the government chooses to employ. This means that states have the power to implement monitoring regimes in ways that are more or less intrusive—and thus more or less constitutionally reasonable—both currently and in response to future technological advances. For example, the visibility of a monitoring device is a function of its size, shape, location, and distinctive configuration. A GPS-based monitoring device that approximates a wristwatch, such as those popular with long-distances runners, may be less obvious, and thus less a brand of criminality, than a traditional ankle monitor—even if an offender cannot remove it. Similar benefits may be achieved by using of devices that may be worn around parts of the body more frequently covered with clothing, such as the bicep or sternum. Reducing or eliminating visible light and audible alerts may help to minimize the attention a monitoring device draws. Not to be overlooked, increasing the reliability of the devices used may result in reducing the police presence at the subject's home, due either to the need for maintenance or to false alerts.[196] Certainly these, and other, advances are already possible.

---

194. Riley v. N.J. State Parole Bd., 98 A.3d 544, 559 (N.J. 2014).

195. The constitutional guarantee of Due Process similarly restricts the government from bringing an ordinary criminal defendant to trial in shackles or prison garb, as these trappings unavoidably and impermissibly connote guilt and dangerousness to the jury. *See* Deck v. Missouri, 544 U.S. 622, 627 (2005); Estelle v. Williams, 425 U.S. 501, 504–05 (1976).

196. Device unreliability can also create spectacle outside of the home. For example, some monitored individuals have described their devices losing signal in large buildings, requiring them to abruptly depart in the middle of activities or transactions in order to

We readily admit that the Fourth Amendment does not require the use of the best-available or least intrusive technology. The touchstone, as always, is reasonableness. At the same time, courts faithful to the spirit of the Fourth Amendment should be particularly wary of governmental choices that seem to be *inviting* spectacle. The history of the public pillory is not so far behind us. Indeed, it was not so long ago that someone thought it wise to invite the media into someone else's private home. To ignore or minimize this dimension of intrusion in the context of technological monitoring, even for convicted sex offenders, would be to undermine the privacy secured by the Fourth Amendment.

IV. ANTICIPATING END-RUNS: IS *GRADY* FACT-BOUND?

The foregoing analysis makes the case that the Fourth Amendment should meaningfully inform how technology is deployed in monitoring sex offenders. Before concluding, we also want to briefly anticipate and address two potential legislative choices that might be viewed as ways around the constraints on monitoring imposed by the Fourth Amendment. Ironically, these choices operate by dispensing with any characterization of technological monitoring as purely civil, a characterization that has frequently insulated sex offender laws from challenge under other constitutional provisions. These seemingly easy "solutions" will undoubtedly occur to some legislators—perhaps those seeking to preserve the status quo in the face of technological advances capable of reducing the invasion experienced by released sex offenders, or perhaps those seeking to implement even more invasive technologies for other, potentially punitive, purposes. Upon inspection, neither "solution" seems likely to permit a complete end-run of the Fourth Amendment's requirement of reasonableness as it applies to technological monitoring regimes. In fact, closer scrutiny suggests they may be much less successful than one might initially imagine.

---

re-establish the lost connection. *See* Brief for the ACLU of Mich. and the Crim. Def. Atty's of Mich. as Amici Curiae, *supra* note 97, at *App'x. It goes without saying that the possibility of such a revealing occurrence is likely to chill the offender's willingness to engage in these everyday social (and often essential) activities in the first place.

A. Imposing Monitoring as a Punishment

The first potential end-run occurs when governments decide to impose technological monitoring on sex offenders as part of the explicit punishment for their crimes. A number of states currently have laws permitting or requiring monitoring as a part of the sentence for at least some subset of sex offenses. A quintessential example is Michigan, which statutorily mandates lifetime electronic monitoring for anyone convicted of a first- or second-degree sex offense involving a child under the age of 13.[197] The Supreme Court has repeatedly announced that prisoners have a drastically diminished expectation of privacy compared to ordinary citizens.[198] One might therefore assume that imposing electronic monitoring as a kind of "technological incarceration" will permit a much greater level of intrusion by virtue of the weakened Fourth Amendment interests at stake under these circumstances. In addition, there may be an inclination to discount the intrusion of technological monitoring by comparing it to the intrusion of incarceration as an alternative punishment.[199] In fact, Judge Posner made a similar argument in upholding Wisconsin's *civil* monitoring program in *Belleau*.[200]

This argument turns out to be much weaker than it might appear, however. There is nothing talismanic about labeling a search a "punishment" that automatically diminishes the privacy interests of the person being searched. The Supreme Court's proclamations that *prisoners* have a reduced privacy interest are the result of a practical determination about the realities of custodial incarceration. For example, the Court famously announced in *Hudson v. Palmer* that "the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell."[201] Yet it is clear that this conclusion followed from the fact that recognizing a right of privacy in a cell—perhaps the only place inmates can reliably conceal contraband, including weapons—would render the

197. *See* MICH. COMP. LAWS § 750.520n(1) (2006).

198. *See, e.g.*, Hudson v. Palmer, 468 U.S. 517, 526 (1984).

199. *See, e.g.*, Bagaric, Hunter, & Wolf, *supra* note 4, at 125 (explaining that monitored offenders have increased privacy because, "unlike the inmates of many conventional prisons, they will be free to shower, use the toilet, and participate in other daily activities unscrutinized by others").

200. *Belleau*, 811 F.3d at 932.

201. *Hudson*, 468 U.S. at 526.

already extraordinarily difficult undertaking of prison administration "literally impossible."[202] In the same opinion, the Court reiterated its continued insistence "that prisoners be accorded those rights not fundamentally inconsistent with imprisonment itself or incompatible with the objectives of incarceration."[203] In other words, stripping prisoners of certain Fourth Amendment protections is done precisely and only because it is necessary to effectuate reasonable incapacitation.[204]

Moreover, when the Fourth Amendment does apply to those in prison custody, it applies in the ordinary way. A recent opinion from the same Term in which the Court announced *Jones* demonstrates this principle. Albert Florence, arrested on an erroneous bench warrant for failing to pay a court fine, was subjected to two separate strip searches as part of the intake process at two New Jersey correctional facilities.[205] According to Florence, the searches involved (among other things) his completely disrobing, opening his mouth and lifting his tongue for inspection, lifting his genitals, and coughing in a squatting position.[206] The Supreme Court was sharply divided over whether such an extensive search was reasonable, given that there was no reason to suspect that Florence would be concealing contraband.[207] (There was no debate that a search had occurred.) The Fourth Amendment framework employed by the Court was the same familiar reasonableness standard employed outside prison walls: "The need for a particular search must be balanced against the resulting invasion of personal rights."[208] Although the Court ultimately held that the needs of preventing contraband from entering the general jail population outweighed the indignity of the search, Justice Kennedy's opinion hinted that the outcome could easily have been different had either the government's interest been less substantial (as in the case of prisoners held in isolation) or

202. *Id.* at 527.

203. *Id.* at 523.

204. We acknowledge, of course, that the diminution of privacy experienced by prisoners may also incidentally serve retributive goals. However, we do not read the Court's jurisprudence to suggest that the reduction in Fourth Amendment protection is itself *a part of* the punishment imposed, rather than merely incidental to a lawful punishment.

205. Florence v. Bd. of Chosen Freeholders, 566 U.S. 318, 323 (2012).

206. *Id.* at 323–24.

207. The Court divided 5–4, and Justice Breyer wrote a strongly worded dissent emphasizing the humiliation and degradation involved in body cavity searches. *See id.* at 342 (Breyer, J., concurring).

208. *Id.* at 327 (majority opinion).

the invasiveness of the search been more significant (as in the case of a search involving physical touching).[209]

Crucially, Albert Florence's case illustrates that all Fourth Amendment searches—even those of prisoners—must be tailored to the government's legitimate aims. It is here that the end-run meets its end. With one notable exception, we can think of few arguments that meaningfully distinguish the purposes of technological monitoring, when imposed as a punishment for a crime, from those of the same monitoring when imposed as a form of civil protection, at least with respect to the same individual.[210] Under either monitoring regime, the primary purpose of monitoring is to deter future criminality by increasing the probability of detection. Any other purposes can be achieved more effectively via other means (e.g., a scarlet letter). Because increasing the probability of detection is accomplished through the collection of information, the "search" that is monitoring should be tailored to be only as intrusive as necessary to collect the pertinent information in a manner that supports the goal of deterrence.

It is theoretically possible that the use of more intrusive technology—a more physically taxing device, or a device that collects more or more intimate information than needed to deter—would also have some small general deterrent effect. We strain to imagine, however, a straight-faced constitutional advocate arguing to a court that the Fourth Amendment does not prohibit an otherwise unreasonable search because the government receives such an attenuated benefit from the most egregious intrusions.[211] The argument proves far too much and would rob the Fourth Amendment of nearly any bite. As the aims of both civil and punitive technological monitoring very nearly converge, the reasonableness

209. *See id.* at 338–39.

210. The exception is the intrusion of public stigma. In Part III.D, we concluded that the goals of a civil sex offender monitoring regime are not furthered by a search that invites public stigma. However, shaming punishments have seen a resurgence of interest in recent years, notwithstanding their questionable efficacy and policy. *See generally* James Q. Whitman, *What is Wrong with Inflicting Shame Sanctions?*, 107 YALE L.J. 1055, 1057 (1998). It is at least plausible that a legislature could choose to impose technological monitoring as a punishment in a manner that invites stigmatization and social castigation. However, if these were the goals, they could be accomplished much more effectively as a separate category of punishment, one that sends clearer signals, is less costly to maintain, and so on.

211. On that logic, the Fourth Amendment would likewise have nothing to say about imposing a daily strip search as a punishment for a non-contraband crime, such as tax evasion.

requirements of the Fourth Amendment should be quite similar regardless of how the statute is labelled.

B. Requiring Consent to Monitoring as a Condition of Parole or Probation

A second anticipated legislative end-run around the Fourth Amendment occurs when governments require that offenders consent to monitoring as a condition of their parole or probation. Currently, several states already approach monitoring in this way. Tying technological monitoring to parole or probation might be thought to weaken claims of intrusiveness in two separate ways. First, it could undermine the weight of the offender's privacy interests in the evaluation of whether the search was unreasonable. The Supreme Court has repeatedly stated that parolees and probationers exist along a spectrum of diminished privacy that includes prisoners at one extreme and ordinary citizens at the other. The Supreme Court has invoked this rationale twice this century, first to uphold the warrantless search of a probationer in *United States v. Knights*,[212] and subsequently to uphold the warrantless search of a parolee in *Samson v. California*.[213] Second, if technological monitoring is a condition of parole or probation, the search effected by that monitoring is arguably consensual. Consensual searches are a well-established exception to the Fourth Amendment's requirements of a warrant and probable cause.[214] Indeed, Judge Posner in *Belleau* anticipated this tactic and described it as an "unassailable" legislative response that would have given the plaintiff in that case a hollow victory on Fourth Amendment grounds.

We can dispense with the first part of the argument relatively quickly, however, as the same logic that applies to prisoners applies with perhaps greater force to probationers and parolees. Neither *Knights* nor *Samson* held that a person's penal status alone permits a level of intrusion comparable to the constant electronic surveillance experienced by monitored sex offenders. Rather, as always, the intrusion into privacy must be justified by the goals to be served, including the reintegration of the offender

212. *Knights*, 534 U.S. 112 (2001).

213. *Samson*, 547 U.S. 843 (2006).

214. Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 FLA. L. REV. 509, 512 (2015).

into society and the protection of the community. In fact, *Knights* held only that a one-time, warrantless search of a probationer's apartment was reasonable when it was supported by individualized suspicion that a probation violation had occurred.[215] The Supreme Court left open the question whether the search of a probationer could ever be reasonable absent individualized suspicion.[216]

Samson, by contrast, did uphold the suspicionless search of a parolee (who, by virtue of that status, had less of an expectation of privacy than a probationer).[217] Parole may therefore provide a firmer legal foothold for suspicionless technological monitoring of sex offenders. However, the *Samson* Court was explicit that the government did not have "a blanket grant of discretion untethered by any procedural safeguards":[218]

> The concern that California's suspicionless search system gives officers unbridled discretion to conduct searches, thereby inflicting dignitary harms that arouse strong resentment in parolees and undermine their ability to reintegrate into productive society, is belied by California's prohibition on "arbitrary, capricious or harassing" searches. The dissent's claim that parolees under California law are subject to capricious searches conducted at the unchecked "whim" of law enforcement officers ignores this prohibition.[219]

At first blush, the *Samson* Court's reliance on a state-level policy prohibiting arbitrary, capricious, or harassing searches seems to be cold comfort for parolees. But consider the contrast being drawn here, and its implications for the reasonableness of technological monitoring. If the dividing line between constitutional and unconstitutional searches of parolees is caprice—unchecked whims, unbridled discretion—what are we to make of monitoring technologies that subject a person to *constant* surveillance, that record and store the results of that surveillance for some indefinite future use? As we previously discussed in connection with the mosaic

---

215. *Knights*, 534 U.S. at 121.

216. *Id.* at 120 n.6 ("We do not decide whether the probation condition so diminished, or completely eliminated, Knight's reasonable expectation of privacy . . . that a search by a law enforcement officer without any individualized suspicion would have satisfied the reasonableness requirement of the Fourth Amendment. The terms of the probation condition permit such a search, but we need not address the constitutionality of a suspicionless search because the search in this case was supported by reasonable suspicion.").

217. *Samson*, 547 U.S. at 856.

218. *Id.* at 856 (quoting Stevens, J., dissenting).

219. *Id.*

theory of the Fourth Amendment, the aggregation of data from a constant technologically enhanced search program is likely to be viewed differently by a court than an examination of any single search. *Samson* thus suggests that the Fourth Amendment may in fact continue to be a source of meaningful pushback to the implementation of technological monitoring, even with respect to parolees and their diminished privacy expectations.

The issue of consent, however, is murkier. To date, the Supreme Court has explicitly avoided the question whether an individual can consent to suspicionless searches as a condition of probation or parole.[220] The notion that a probationer or parolee consents to technological monitoring as a condition of release may hold intuitive appeal. After all, "consent search" programs are a common facet of everyday life—at least for anyone who has flown on an airplane recently.[221] In contexts such as air travel, we see consenting to governmental searches as a worthwhile price in exchange for certain liberties. However, the legal issue is actually quite a bit more complicated with respect to probationers and parolees (undoubtedly a reason why the Supreme Court has so far punted). The Supreme Court has explained that consensual searches are evaluated under the same constitutional standard as voluntary confessions—that is, they must be free from the taint of duress or coercion, whether express or implied.[222] Even if parolees or probationers have the choice to opt for incarceration,[223] there are substantial arguments to be made that the conditions of such choice are coercive, and thus the consent offered is not truly voluntary. Indeed, the Ninth Circuit has long held that the government may never induce consent to an unreasonable search by making it a condition of probation because "there is a limit on the price the government may exact" for freedom.[224] Ultimately, the voluntariness of consent is a question of fact to be determined from the full panoply

220. *See id.* at 852 n.3; *Knights*, 534 U.S. at 118.

221. *See* United States vs Davis, 482 F.2d 893, 908 (9th Cir. 1973).

222. Schneckloth v. Bustamonte, 412 U.S. 218, 248 (1973).

223. Many do not. In some states, parole is imposed unilaterally and the offender has no option of remaining incarcerated if he or she disagrees with the parole conditions. To speak of "consent" to search in those circumstances would be to engage in the most unhelpful kind of legal fiction.

224. United States v. Lara, 815 F.3d 605, 609 (9th Cir. 2016) (discussing United States v. Consuelo-Gonzalez, 521 F.2d 259, 261 (9th Cir. 1975) (en banc)). But, of course, this is an unsettled question, and some courts have in fact found voluntary consent in similar circumstances. *See, e.g.*, United States v. Yeary, 740 F.3d 569, 583 (11th Cir. 2014) (finding voluntary, uncoerced consent to warrantless searches as a condition of pre-trial release).

of circumstances, including whether the suspect knows that he has a right to refuse.[225] Thus the effectiveness of this strategy as a potential end-run around the Fourth Amendment is far from obvious.

CONCLUSION

The Fourth Amendment's command of reasonableness calls for balancing two sets of weighty interests. There is no easy answer to the question when a proper balance has been struck. A crucial first step is to identify the relevant factors that comprise those interests so that they can be fairly assessed. An important goal of this Essay has been to disaggregate the key dimensions of intrusiveness of technological monitoring, particularly in the case of convicted sex offenders who are facing monitoring for many years or life. Notwithstanding our disaggregation, the Fourth Amendment reasonableness inquiry is always an assessment of the totality of the circumstances.

We can imagine different ways that this plays out in litigation. On the one hand, courts may employ an arithmetical model of intrusion, finding that a state's chosen monitoring technology is reasonable whenever the aggregate intrusion is below a particular threshold. On this model, courts may tolerate a high level of intrusion along one or more dimensions, provided that those intrusions are offset by sufficiently minor intrusions along other dimensions. Alternatively, the realities of litigation may tend to drive courts' attention to the most egregious intrusions. As a result, courts may naturally gravitate toward a low-variance model of reasonableness that seeks to minimize outliers, even if it means a higher level of citizen intrusion in the aggregate. Either way, we believe that policymakers seeking to design and enforce a monitoring regime that respects the law and the spirit of the Fourth Amendment will find guidance in this Essay. At the same time, by identifying the Fourth Amendment pressure points of monitoring, we hope that we have provided advocates and reformers with at least some grist for the mill when they run headlong into monitoring regimes that are unnecessarily or arbitrarily burdensome. Technological monitoring can be tailored to fit the characteristics and circumstances of individual convicted sex offenders and, in so doing, reduce the intrusiveness of the search, just as the Fourth Amendment entreats the government to do.

---

225. *Schneckloth*, 412 U.S. at 248–49.