CARDOZO LAW REVIEW
de•novo

"MOSAIC THEORY" AND MEGAN'S LAWS

*Wayne A. Logan**

In law as in life, a change in perspective can sometimes afford an opportunity to conceive of a once settled matter in a new, more meaningful way. Such an opportunity is now presented by the D.C. Circuit's recent decision in *United States v. Maynard*,[1]which held that the Fourth Amendment is violated when police, acting without a search warrant, make prolonged use of Global Positioning System (GPS) technology to create a "mosaic" of information of an individual's public travel by car. The decision, authored by one of the nation's best known conservative jurists, Douglas Ginsburg,[2] created a circuit split that the Supreme Court has agreed to resolve (docketed *sub nom. United States v. Jones*).[3]

---

*Gary & Sallyn Pajcic Professor of Law, Florida State University College of Law. Thanks to Susan Bandes, David Logan, Dan Markel, Chris Slobogin, and Ron Wright for their helpful comments.

1 615 F.3d 544 (D.C. Cir. 2010), *reh'g denied sub nom*. United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *cert. granted*, No. 10-1259, 79 U.S.L.W. 3610 (June 27, 2011).

2 *See* 2 ALMANAC OF THE FEDERAL JUDICIARY 9-12 (2010 ed.) (noting Judge Ginsburg's appointment to D.C. Circuit by President Reagan and unsuccessful nomination to Supreme Court by President Bush (I)). The other two panel members, Judges David Tatel and Thomas Griffith were nominated by Presidents Clinton and Bush (II). *Id.* at 12-14 (Griffith); *id*. at 19-22 (Tatel). For evidence that Judge Ginsburg is not alone among judicial conservatives in his privacy concern over prolonged GPS monitoring in public spaces see, e.g., United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc) (noting that "there's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention.").

3 *See, e.g.,* United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011) (finding no violation, over extended dissent of Judge Wood); United States v. Marquez, 605 F.3d 604 (8th Cir. 2010) (finding no violation); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (finding no violation); United States v. Narrl, No. 2:09–992, 2011 WL 1597662 (D. S.C. Apr. 27, 2011) (same but offering that "[m]uch of the reasoning in *Maynard* is attractive."). In addition, several state courts have deemed prolonged warrantless GPS surveillance as searches violative of their state constitutions. *See* Comm. v. Connolly, 913 N.E.2d 356 (Mass. 2009); People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009); State v. Holden, No. 1002012520, 2010 WL 5140744 (Del. Super. Ct., Dec. 14, 2010). In its *certiorari* grant, the Court agreed to answer whether warrantless use of the GPS device constituted a search in violation of the Fourth Amendment, and directed the parties to also address whether installation of the device on Jones's vehicle violated the Fourth Amendment. *See* United States v. Jones, No. 10-1259, 79 U.S.L.W. 3610 (June 27, 2011).

Time will tell whether *Maynard*'s view of the transformative effect of technology, as a collector and aggregator of publicly available facts, will be a watershed event akin to *Katz v. United States*,[4] which emancipated Fourth Amendment doctrine from physical entry and property interests. It certainly has the potential to do so.[5]

Meanwhile, the approach in *Maynard* affords a new way to assess the constitutionality of yet another government data collection and aggregation enterprise—registration and community notification (RCN), commonly known as Megan's Laws.[6] In effect nationwide since the late 1990s, RCN requires that ex-offenders, typically convicted of a sex offense, provide government authorities with information regarding where they live, attend school and work; any vehicle(s) they drive; their physical characteristics (such as birthmarks and tattoos); facial photos; and criminal histories. The information, which must be verified at specified intervals, and updated in the event of any changes, for a minimum period of ten years and often for registrants' lifetimes, is then disseminated world-wide (via the Internet) in the name of promoting public safety.[7]

Registry information, like the travel in *Maynard*, is of course "public" in a most basic sense. Yet it is also the case that—without government enterprise—the individual data bits collected in both contexts would be beyond the practical reach of others. Just as the practical limits of surveillance capacity and resources preclude police from continuous month-long monitoring of a suspect's car travel, governments (and community members) lack the capacity to gather comprehensive and current identifying information on registrants. And, critically important, even if such data were somehow collected, they would remain disaggregated and not create informational mosaics revealing the daily existence of targeted individuals.

This Essay applies the crucial insight of *Maynard*, that aggregated publicly available data can raise a Fourth Amendment privacy concern,

---

4 389 U.S. 347, 351-52 (1967).

5 *See, e.g.,* Adam Liptak, *Court Case Asks if "Big Brother" Is Spelled GPS*, N.Y. TIMES, Sept. 10, 2011, at A1 (calling *Maynard* "the most important Fourth Amendment case in a decade.").

6 The reference stems from the July 1994 sexual assault and murder of seven-year-old Megan Kanka, which prompted the New Jersey Legislature to adopt by unanimous vote a registration and community notification law a few months later. New Jersey's law, while not the nation's first RCN provision, served as a major social and political catalyst, and "Megan's Laws" has since served as an eponymous short-hand reference for RCN laws more generally. *See* WAYNE A. LOGAN, KNOWLEDGE AS POWER: REGISTRATION AND COMMUNITY NOTIFICATION LAWS IN AMERICA 54-55 (Stanford Univ. Press, 2009) [hereinafter LOGAN, KNOWLEDGE AS POWER].

7 *See id.* at 66-81. RCN coverage actually extends well beyond sex offenders, ranging from child kidnappers to public urinators, and its appeal as a low-cost community-based social control method (compared to prison) is evident in its continued expansion. *See id.* at 73-74, 178-79; Erica Goode, *States Seeking New Registries for Criminals*, N.Y. TIMES, May 20, 2011, at A1 (noting extension *inter alia* to persons convicted of homicide and likening new laws to "Christmas ornaments on a tree, [added] year after year.").

to the question of whether RCN implicates a protectable Fourteenth Amendment substantive due process privacy interest.[8] Part I summarizes the facts and holding of *Maynard*. Part II surveys the case law, dating back to the mid-late 1990s, addressing privacy challenges to RCN, which typically found no such interest to exist. Part III examines the question anew, applying mosaic theory to conclude that RCN does indeed affect the privacy interests of the over 700,000 individuals it now targets.

This recognition, however, constitutes only a first step in the analysis. Courts would then need to address whether RCN's negative effects on privacy outweigh its avowed public safety purpose.[9] When they do so, they will need to weigh the growing body of research casting significant doubt on the efficacy of RCN. Odds are, given the deference typically afforded exercises of state police power such as RCN, and the laws' continued political popularity, such a challenge will ultimately fail. Nevertheless, as discussed later, the evaluative process necessitated will itself have significant benefit, for the first time requiring government to account for the negative privacy consequences of its sustained, information-based public safety experiment.

I. MAYNARD

In *Maynard*, District of Columbia police suspected that Lawrence Maynard and co-defendant Antoine Jones were engaged in a conspiracy to traffic cocaine, and despite lacking a lawful search warrant,[10] affixed a GPS tracking device to Jones's vehicle and tracked its location twenty-four hours a day for twenty-eight days. Police then used the information obtained—a pattern of visits to a known drug stash house—to convict him of drug conspiracy charges at trial.[11] The D.C. Circuit reversed the trial court's denial of Jones's motion to suppress the GPS evidence, concluding that the prolonged and continuous use of the tracking device qualified as a search, violating his reasonable expectation of privacy under the Fourth Amendment.[12]

In reaching its result, the *Maynard* court needed to reconcile accepted Fourth Amendment wisdom that no privacy expectation

---

[8] For similar prior efforts to draw connective doctrinal lessons from distinct constitutional areas *see, e.g.*, David Cole, *The Value of Seeing Things Differently;* Boerne v. Flores *and Congressional Enforcement of the Bill of Rights*, 1997 SUP. CT. REV. 31; Tracey Maclin, *What Can Fourth Amendment Doctrine Learn from Vagueness Doctrine?*, 3 U. PA. J. CONST. L. 398 (2001).

[9] *Cf.* Akhil Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 811 (1994) (noting parallel reasonableness inquiries in Fourth and Fourteenth Amendment).

[10] Police obtained a warrant to install the device in the District of Columbia but actually installed it in Maryland after the warrant expired. *Maynard*, 615 F.3d at 566 FN*.

[11] *Id.* at 567-68.

[12] *Id.* at 568.

attaches to anything "a person knowingly exposes to the public,"[13] and *United States v. Knotts,*[14] which held that implanting a beeper device in a container of chemicals, and tracking the container as it was transported in a car driven 100 miles on public roads, did not qualify as a search.[15] Seizing on the fact that *Knotts* reserved judgment on whether "dragnet-type," "twenty-four hour surveillance" might constitute a search,[16] the *Maynard* court distinguished *Knotts*, noting that Jones was in fact subject to twenty-four hour surveillance and for an extended period of time (as opposed to a single discrete trip).[17]

The court next considered whether the totality of Jones's movements was subjectively "exposed" to the public—either actually or constructively—sufficient to preclude any Fourth Amendment privacy expectation.[18] As to actual exposure, the court stated that the likelihood that "the whole of one's movements over the course of a month" being actually exposed to others was "effectively nil."[19] Framing the issue in terms of what police "might actually do," not what they "could have done," consistent with the Supreme Court's decision in *Bond v. United States*,[20] the court wrote that

> [i]t is one thing for a passerby to observe or even follow someone during a single journey . . . . It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[21]

Turning to the possibility of constructive exposure, the court posited that "[w]hen it comes to privacy . . . the whole may be more revealing than the parts,"[22] citing two Supreme Court cases in support. In the first, *United States Department of Justice v. Reporters' Committee for Freedom of the Press*,[23] arising in response to a Freedom of Information Act request, the Court held that a privacy right exists in a "rap sheet," containing an individual's criminal history information,

---

13 *Katz*, 389 U.S. at 351.

14 460 U.S. 276 (1983).

15 *Id.* at 281 (stating that travel on public roads itself "voluntarily conveyed to anyone who wanted to look" the car's route and destination).

16 *Id.* at 283-84 (stating that "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

17 United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

18 *See Katz*, 397 U.S. at 360-61 (Harlan, J., concurring) (conceiving now-dominant two-part test asking whether individual exhibited an actual, subjective expectation of privacy and whether the expectation was objectively reasonable by societal standards).

19 *Maynard*, 615 F.3d at 558.

20 *Id.* at 560 (citing United States v. Bond, 529 U.S. 334 (2000)).

21 *Id.*

22 *Id.* at 561.

23 489 U.S. 749 (1989).

date of birth, and physical description. While the individual criminal event records were indeed public, individuals had a privacy interest "in the aggregated 'whole' distinct from their interest in the 'bits of information' of which it was composed."[24] The second decision, *Smith v. Maryland*,[25] involved the government's use of a pen register to collect numbers dialed from a criminal suspect's phone without a warrant. While *Smith* held that doing so did not violate the suspect's reasonable expectation of privacy under the Fourth Amendment, it implicitly recognized the significance of data aggregation insofar as the suspect dialed the numbers knowing that his phone company could and did in fact record all numbers accessed (as indicated on his bill), defeating any privacy expectation with regard to any pattern thereby created.[26]

In both *Reporters' Committee* and *Smith*, data aggregation, like the government's use of mosaic theory in national security information cases,[27] created a difference not "of degree but of kind."[28] "The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet," the court concluded, "that whole reveals far more than the individual movements it comprises."[29] Aggregated travel data enables inferences to be drawn based on repetition or sequencing, potentially revealing such matters as whether a person "is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[30]

The *Maynard* court then addressed the second prong of the *Katz* test—whether the prolonged use of GPS violated an objective, societal expectation of privacy. Again, the court found in the affirmative, citing state laws prohibiting private citizens from using electronic tracking devices, and the resource and practical obstacles precluding police from actually undertaking month-long visual surveillance. With respect to the latter in particular, the court observed that "[c]ontinuous human

---

[24] *Maynard*, 615 F.3d at 561 (quoting *Reporters' Committee*, 489 U.S. at 764). In a footnote, the court elaborated that

> [t]he colloquialism that "the whole is greater than the sum of its parts" is not quite correct. "It is more accurate to say that the whole is something different than the sum of its parts." Kurt Koffka, Principles of Gestalt Psychology 176 (1935). That is what the Court was saying in *Reporters' Committee* and what we mean to convey throughout this opinion.

Id. at 561 FN*.

[25] 442 U.S. 735 (1979).

[26] *Maynard*, 615 F.3d at 561 (citing *Smith*, 442 U.S. at 742-43, 745).

[27] *See id.* at 562 ("As with the 'mosaic theory' often invoked by the Government in cases involving national security information, 'What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.' CIA v. Sims, 471 U.S. 159, 178 (1985)").

[28] *Id.*

[29] *Id.*

[30] *Id.*

surveillance for a week would require all the time and expense of several police officers, while comparable photographic surveillance would require a net of video cameras so dense and so widespread as to catch a person's every movement, plus the manpower to piece the photographs together."[31] Use of GPS technology did not face similar constraints; not only was installation of the device itself easy, but extending the period of GPS surveillance indefinitely was effectively cost-free.[32] "For these practical reasons," the *Maynard* court concluded, "the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave."[33]

II. RCN AND PRIVACY IN THE COURTS

To date, privacy-based challenges against RCN have met near-uniform resistance from state and federal courts. Among the most influential such decisions is *Russell v. Gregoire*,[34] where the Ninth Circuit upheld Washington State's RCN scheme, adopted in 1990 and amended at various points through 1996. In Washington, individuals were required to provide authorities their name; current home address and place of employment; date and place of birth; crime of conviction and time and place of occurrence; social security number; photograph; and fingerprints.[35] Photos, conviction histories, and approximate residential locations of those individuals thought to pose the greatest risk of recidivism were then disclosed by means of community notification meetings conducted by police.[36]

Subsequent to registering, two convicted sex offenders sued to enjoin release of the information, alleging *inter alia* that Washington's law violated their Fourteenth Amendment substantive due process right to privacy. The Western District of Washington denied their request for injunctive relief yet stayed community notification pending appeal.[37]

The Ninth Circuit rejected the claim, stating that "any such right to privacy, to the extent it exists at all, would protect only personal information," such as that of a medical nature.[38] RCN information, the court wrote, was "already fully available to the public and is not constitutionally protected . . . with the exception of the general vicinity of the offender's residence (which is published) and the offender's employer (which is collected but not released to the public). Neither of

---

31 *Id.* at 565.
32 *Id.*
33 *Id.*
34 124 F.3d 1079 (9th Cir. 1997).
35 *Id.* at 1082.
36 *Id.*
37 *Id.* at 1083.
38 *Id.* at 1094 (citing Whalen v. Roe, 429 U.S. 589, 599 (1977)).

these items are [sic] considered private."[39]

More recent challenges brought against newer laws, requiring disclosure of more detailed information—including specific home addresses (often indicated by pinpoint maps), as well as places of employment and vehicle descriptions—have also been unsuccessful. This is because, again, the individual pieces of identifying information are "public" in nature.[40] In *Doe v. Kelly*, for instance, the Western District of Michigan summarily refused to find a privacy right sufficient to "prevent[] compilation and dissemination of truthful information that is already, albeit less conveniently, a matter of public record."[41] More recently, in *Smith v. Doe*[42] the U.S. Supreme Court endorsed a similarly narrow understanding in its rejection of a claim that Alaska's RCN law qualified as retroactive punishment in violation of the Ex Post Facto Clause. According to the Court, the law merely allowed for "dissemination of accurate information about a criminal record, most of which is already public."[43] The state's online registry was like a "visit to an official archive of criminal records," simply made "more efficient, cost effective, and convenient for Alaska's citizenry" as a result of being on the Internet.[44]

III. MOSAIC THEORY AND RCN

Maynard is surely susceptible to critique, for practical reasons if none other. How and where, for instance, is the line to be drawn—when is a "mosaic" created sufficient to qualify as a "search" triggering the Fourth Amendment?[45] Nevertheless, *Maynard* represents an important departure from the cramped public/private rubric that has long dominated Fourth Amendment analysis, attaching significance to how data aggregation impacts privacy, even when the individual data

---

39 *Id.*

40 *See, e.g.,* Doe v. Moore, 410 F.3d 1337, 1345 (11th Cir. 2005) (concluding that "a state's publication of truthful information that is already available to the public" does not infringe a privacy right); Hyatt v. Comm., 72 S.W.3d 566, 574 (Ky. 2002) ("The information is not truly personal data…because convicted sex offenders never had a reasonable expectation of privacy in regard to the information that is now consolidated and posted on the sex offender registry.").

41 961 F. Supp. 1105, 1112 (W.D. Mich. 1997); *see also, e.g.,* People v. Logan, 705 N.E.2d 152, 160 (Ill. Ct. App. 1999) (registration "merely compiles truthful, public information, and the Notification Law makes this information more readily available."); State v. Williams, 728 N.E.2d 342, 356 (Ohio 2000) ("Active distribution, as opposed to keeping open the doors to government information, is a distinction without significant meaning. The information at issue is a public record, and its characteristic as such does not change depending on how the public gains access to it.").

42 538 U.S. 84 (2003).

43 *Id.* at 99.

44 *Id.* at 100.

45 This notwithstanding the fact that arbitrarily set temporal bounds are of course not unusual in constitutional criminal procedure more generally. *See, e.g.,* Maryland v. Shatzer, 130 S. Ct. 1213, 1223 (2010) (designating 14 days as the point when a suspect's prior invocation of *Miranda* counsel right lapses, allowing police to re-approach suspect).

bits themselves are as a technical matter publicly available.

Like single brush strokes in a Pointillist or Impressionist painting, assembling publicly available data can have a transformative effect. It is not the case, as dissenting members of the D.C. Circuit asserted in an unsuccessful effort to have *Maynard* reheard *en banc*, that "[t]he sum of an infinite number of zero-value parts is also zero."[46] Rather, the data points, when combined and connected, undergo a transformation in form. The Supreme Court spoke to this difference in *Reporters' Committee* in 1977, rejecting a FOIA request for individuals' rap sheet information. Even though conviction "information is a matter of public record," the Court held, "plainly there is a vast difference between the public records that might be found after a diligent search" of government files and the "summary located in a single clearinghouse of information."[47] Indeed, if the information were readily available, the Court reasoned, there would be no need for the rap sheet request in the first instance.[48]

The same observations apply to RCN, which aggregates current home and work address information, where one attends school, and conviction history, perhaps available in far-flung data sources, and current physical trait information and photos, which would likely not be so readily accessible, and publicly disseminates the information. In 1995, the New Jersey Supreme Court embraced mosaic theory, albeit not in name, to find a protectable Fourteenth Amendment privacy interest in RCN information. Even though registrants had no privacy expectation "in many of the individual pieces of information disclosed,"[49] the court held, RCN linked "various bits of information . . . that otherwise might remain unconnected. . .,"[50] creating a "totality of

---

46 United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting from denial of rehearing en banc, joined by Henderson, Brown, and Kavanaugh, J.J.).

47 *Reporters' Committee*, 489 U.S. at 763.

48 *Id.* at 764.

49 Doe v. Poritz, 662 A.2d 367, 408 (N.J. 1995).

50 *Id.* at 411. As the court noted:

> Government dissemination of information to which the public merely has access through various sources eliminates the costs, in time, effort, and expense that members of the public would incur in assembling the information themselves. Those costs, however, may severely limit the extent to which the information becomes a matter of public knowledge. [RCN] therefore exposes various bits of information that, although accessible to the public may remain obscure. Indeed, …if the information disclosed under the Notification Law were, in fact, freely available, there would be no need for the law.

Id. See also Doe v. Biang, 494 F. Supp. 2d 880, 892 (N.D. Ill. 2006) ("it is obvious that aggregated data about sex offenders—which exposes and links pieces of data and aspects of a sex offender's life that otherwise would remain obscure and unconnected–is materially more meaningful than any individual piece of data. Were that not so, there would be no need for [RCN] because an individual's ability to scour police records and phone books would be sufficient to alert and protect the public.").

information" raising a privacy concern.[51] The lynchpin data point, the court reasoned, was the home address, which altered the quality of the data assemblage as a whole.[52] Providing home addresses, in tandem with stigmatizing criminal history information, subjected individuals to "uninvited harassment"[53] and ensured "that a person cannot assume anonymity . . . preventing a person's criminal history from fading into obscurity and being wholly forgotten."[54]

In short, in both contexts government assemblage of public information negatively affects privacy. With RCN, however, the government behavior raises even greater concern. Whereas in *Maynard* the target of government surveillance was unaware of being monitored, RCN surveillance is purposefully and decidedly overt. The government makes no secret of its desire to instill in registrants a sense of being watched.[55] Individuals are required, under threat of punishment, to provide identifying data, verify it at specified intervals (at least annually), and update it in the event of any changes (e.g., a residential move or growth of a beard) potentially for their lifetimes.[56] As a result, they suffer loss of a key additional trapping of privacy—the autonomous right to control information about oneself,[57] in a context

---

51 *Doe*, 662 A.2d at 408; *see also id.* at 409 ("the totality of the information disclosed to the public…implicates a privacy interest. That the information disseminated…may be available to the public, in some form or other, does not mean that plaintiff has no interest in limiting its dissemination.").

52 *Id.* at 409.

53 *Id.*

54 *Id.* at 411. *See also* Artway v. Att'y Gen., 876 F. Supp. 666, 689 (D. N.J. 1995) ("[RCN] goes well beyond all previous provisions for public access to an individual's criminal history….[R]ather than lying potentially dormant in a courthouse record room, a [registrant's] former mischief…shall remain with him for life, as long as he remains a resident of New Jersey."), *aff'd*, 81 F.3d 1235 (3d Cir. 1996); Boutin v. LaFleur, 591 N.W.2d 711, 718 (Minn. Ct. App. 1999) ("there is a distinct difference between the mere presence of such information in court documents and the active dissemination of such information….").

55 *See* LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 60. For an earlier expression of this desired surveillance effect, see Note, *Criminal Registration Ordinances: Police Control over Potential Recidivists*, 103 U. PA. L. REV. 60, 64 (1954) (citing a Philadelphia detective who favored the local registration law (not also entailing community notification) because it led registrants "to believe that they were under the surveillance of the police department. The registrant's feeling of constant surveillance and obligation to notify the police of any change of address might impose some regimentation….").

56 For extended discussion of this impact, especially relative to whether the effects of RCN impose "custody" sufficient to warrant federal habeas corpus protection, see Wayne A. Logan, *Federal Habeas in the Information Age*, 85 MINN. L. REV. 147, 189-207 (2000). *See also* Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321 (2008) (examining array of emerging technologies used to exercise social control, in lieu of physical incapacitation).

57 *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"); Charles Fried, *Privacy [A Moral Analysis]*, 218, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand Schoeman ed., 1984) (terming privacy "that aspect of social order by which persons control access to information about themselves").

that is anything but value-neutral.[58] And, even more problematic, the compelled information is used, not to connect the dots to permit inferences relating to such matters as medical conditions, sexual preferences, or romantic activities, possibilities highlighted in *Maynard*,[59] but rather to enable harassment and threats to personal well-being,[60] the kinds of harms long recognized as jeopardizing a protectable privacy interest.[61]

Ultimately, it may be that the benefits of RCN laws are worth their cost to individual privacy. Indeed, such has been the conclusion of several courts, including the New Jersey Supreme Court in 1995, which having found that RCN jeopardized privacy, nonetheless concluded that its important public safety purpose outweighed the privacy intrusion, when the law at issue "selectively disclosed" registrant data and "carefully calibrated . . . the need for public disclosure" in terms of individualized registrant risk.[62] As application of mosaic theory makes clear, it is this second-stage question, not whether RCN intrudes on privacy as a threshold matter, which courts should now be addressing.[63]

When they do, they might reach a result different than that earlier reached by the New Jersey Supreme Court. While the government interest behind RCN—the prevention of recidivist sexual offenses—remains compelling,[64] today's RCN laws differ significantly from those

---

58 As Seth Kreimer observed: "[n]o one doubts that Hester Prynne's scarlet letter provided more than neutral information, or that the effort of Senator Joseph McCarthy to 'expose' the background of his political opponents was not simply public education." Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension between Privacy and Disclosures in Constitutional Law*, 140 U. PA. L. REV. 1, 7 (1991).

59 *Maynard*, 615 F.3d at 562.

60 LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 125-29 (surveying negative effects of RCN on registrants); *see also* State v. Bani, 36 P.3d 1255, 1265 (Haw. 2001) ("[P]ublic disclosure may encourage vigilantism and may expose the offender to possible physical violence."); Doe v. Portiz, 662 A.2d 367, 409 (N.J. 1995) (noting risk of "uninvited harassment" resulting from disclosure of registrants' home addresses).

61 *See, e.g.,* Kallstrom v. City of Columbus, 136 F.3d 1055, 1063 (6th Cir. 1998) (finding privacy right implicated by disclosure of police officer homes addresses that created risk to their personal security); *cf.* Thornburgh v. Obstetricians & Gynecologists, 476 U.S. 766 (1986) (expressing concern over harassment of women seeking abortions as a result of government disclosure of their identities); Brown v. Socialist Workers Campaign Comm., 459 U.S. 87, 92 (1982) (worrying about harassment of political contributors as a result of government disclosures); Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058, 1065 (9th Cir. 2002) (disallowing effort by anti-abortion activists to publish on website the names, addresses, photos, and vehicle descriptions of abortion providers, with indications of those murdered and wounded).

62 *See* Doe v. Poritz, 662 A.2d 367, 411-12 (N.J. 1995); *see also* Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (finding privacy interest jeopardized but forgoing analysis based on government's compelling interest in preventing sex offenses).

63 *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-78 (3d Cir. 1980) (setting forth multi-part balancing test to determine whether an individual's privacy interest is outweighed by public interest in disclosure).

64 This notwithstanding the understanding that the prime motivation behind RCN laws--that persons convicted of sex offenses as a group recidivate at higher rates than other subpopulations--lacks empiric justification. *See* LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 98-99

of the 1990s. They assemble and disclose in blunderbuss fashion far more extensive and detailed identifying information for all registrants, not (as in the circa 1995 New Jersey law addressed) merely those believed to pose greatest risk,[65] and, other than ineffectual warnings against public misuse,[66] lack the kind of safeguards deemed important in instances of information disclosure.[67] At the same time, the avowed public safety value of RCN has been undercut by a substantial body of research casting doubt on the efficacy of RCN, raising concern that it actually lessens public safety and creates a false sense of security that drains budgets and distracts from more effective possible interventions.[68]

It may well be that the benefit of having government serve as a data collector, aggregator and disseminator of registrant information is worth the attendant cost; but, then again, it might not.[69] More is required of courts than the reflexive acceptance they've shown to date.[70] Ultimately, as with identifying the bounds of protectable privacy itself, the balancing unavoidably entails a legal, practical, and moral judgment. In an era in which fear of crime, and sexual offending in particular, remains high,[71] and Americans like never before regard a criminal conviction as a perpetual badge of dishonor,[72] the smart money should be on continued judicial validation of RCN laws.[73] However,

---

(discussing studies). The public notice goal of RCN laws has also been criticized for the equally false empiric premise that sex offenses most often are committed by strangers, when studies establish that the vast majority of offenses are committed by persons related to or otherwise know by victims. *Id.* at 99 (same).

65 Itself a matter on which the Supreme Court has expressly reserved opinion. *See* Conn. Dep't of Pub. Safety v. Doe, 538 U.S. 1, 8 (2003) ("express[ing] no opinion as to whether Connecticut's Megan's Law violates principles of substantive due process" because of its breadth of coverage).

66 LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 126-27, 159.

67 *See, e.g.,* Whalen v. Roe, 429 U.S. 589, 594, 605-06 (1977) (noting and attaching importance to limits government placed on public disclosure).

68 *See* LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 110-32 (surveying empirical work done to date); Amanda Y. Agan, *Sex Offender Registries: Fear without Function?*, 54 J. L. & ECON. 207 (2011).

69 *See* Paul P. v. Verniero, 170 F.3d 396, 406 (3d Cir. 1999) (Fullam, J., concurring) (questioning whether the "theoretical and 'feel-good' benefits of Megan's Laws may in the long run be overwhelmed by the law's negative consequences. Statutes enabling, perhaps even encouraging, vigilantism and similar harms, seem utterly at odds with constitutional values.").

70 *See, e.g.,* Doe I v. Phillips, 194 S.W.3d 833, 845 (Mo. 2006) ("The safety of children is a legitimate state interest and the purpose of [RCN] is to 'protect children from violence at the hands of sex offenders.' [RCN] bears a rational relation to this legitimate state interest and is not violative of substantive due process principles.").

71 *See* Sarah Craun & Matthew Theriot, *Misperceptions of Sex Offender Perpetration*, 24 J. OF INTERPERSONAL VIOLENCE 2057, 2057-58 (2009); *Americans Still Perceive Crime as on the Rise*, Nov. 19, 2010, available at http://www.gallup.com/poll/144827/Americans-Perceive-Crime-Rise.aspx.

72 *See* LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 155-56 (tracing shift in sentiment).

73 *See* Edward P. Richards, *The Jurisprudence of Prevention: The Right of Societal Self-Defense Against Dangerous Individuals*, 16 HASTINGS CONST. L.Q. 329, 329 (1989) ("As America moves into the twenty-first century, we must determine to what extent individual

only by frankly and realistically acknowledging that the laws affect privacy will the important public policy debate be able to ensue in earnest.

IV. CONCLUSION

This Essay has applied mosaic theory, a novel Fourth Amendment construct with potentially important implications for government surveillance efforts, to the question of whether registration and community notification laws jeopardize a protectable Fourteenth Amendment privacy interest. Even assuming the nominally public quality of the individual data bits assembled by RCN, such as home and work addresses and current physical descriptions, their aggregation and dissemination creates an informational mosaic of personal existence, which like the travel data in *Maynard* differs in form from what the Supreme Court in *Smith v. Doe* simplistically likened to a "visit to an official archive of criminal records."[74] By the same token, *Maynard,* despite its Fourth Amendment focus*,* highlights the crucial analytic importance of focusing on the actual use of assembled data, rather than merely asking whether particular constituent parts are public or private in an abstract sense, as long urged by privacy proponents.[75]

Institutionally, it will ultimately fall to the courts to effectuate the conceptual transformation urged here. While it has been argued that legislatures hold superior promise to protect privacy in the face of technological advances,[76] little realistic hope exists for a political limit on RCN, given the attendant mortal political risk of appearing indulgent of convicted criminals (especially sex offenders).[77] Whatever the result reached by the Court this Term in *Maynard*, application of mosaic theory highlights the very real effect that RCN has on individual privacy, subject to Fourteenth Amendment protection, obliging a more robust examination of it and other government data aggregation and dissemination strategies likely to emerge in the years to come.

---

liberties must be sacrificed for the common good. Ideals of liberty and privacy are stretched to the limit as modern fears of street crime merge with ancient fears of the plague.").

74 Smith v. Doe, 538 U.S. 84, 100 (2003).

75 *See, e.g.,* Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 980 (1989); Daniel Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1065 (2003).

76 *See, e.g.*, Orin Kerr, *The Fourth Amendment and New Technologies*, 102 MICH. L. REV. 801, 882-87 (2004).

77 *See* LOGAN, KNOWLEDGE AS POWER, *supra* note 6, at 165-71 (surveying reasons for the ongoing political impregnability of RCN laws). Testament to this, many legislatures have seen fit to specify that individuals subject to RCN lack protectable privacy interests. *Id.* at 270 n.87.