PROTECTING PRIVACY WITH FOURTH AMENDMENT USE RESTRICTIONS

Rebecca Lipman[*]

INTRODUCTION

The Fourth Amendment prohibits "unreasonable searches and seizures."[1] Traditionally, the Supreme Court has enforced this prohibition by requiring law enforcement officers to acquire a warrant before conducting a search or seizure, subject to several exceptions.[2] Once a law enforcement officer acquires a warrant and collects the material specified in the warrant, the constitutionality of how officers may *use* that material has not generally been questioned.[3] Anything law enforcement officers do post collection has not traditionally been considered a "search" and therefore is not subject to Fourth Amendment regulation.[4]

This interpretation of the Fourth Amendment as a protection limited only to the initial acquisition of information is unnecessarily narrow. This Article will demonstrate that the Fourth Amendment can, and should, regulate the use of lawfully collected material. Although this application of the Fourth Amendment goes beyond the traditional scope, multiple prior Supreme Court cases reflect this potential where the use of collected material has driven the Court's judgment about the lawfulness of the collection.[5] In one case, the Court outright prohibited a particular use while silently permitting the collection to continue.[6] Without announcing that it has the power to impose use restrictions, the Court has nevertheless moved towards regulating both collection and use under the Fourth Amendment.[7]

It is important to delineate the terms "collection" and "use" in this Article. "Collection" means the act of gathering items or information. This includes physically collecting objects, recording video footage, eavesdropping

---

[*] Assistant Corporation Counsel at the New York City Law Department. J.D. cum laude, Harvard Law School, 2015. Many thanks to Dan Solove, Orin Kerr, Adrian Vermeule, Susan Freiwald, Judge Stephen Smith, Brian Owsley, Stephen Henderson, Kiel Brennan-Marquez, Bryan Choi, Kendra Albert, Debrae Kennedy-Mayo, Christina Black, Marcel Kahan, Ryland Li, Jane Stapleton, Ira Rubinstein, Kaitlin Caruso and the excellent participants at the 2017 Privacy Law Scholars Conference. This Article reflects the author's views alone, and not those of the City of New York or the New York City Law Department.

1 U.S. CONST. amend. IV.

2 *See, e.g.*, Katz v. United States, 389 U.S. 347, 357 (1967).

3 *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 95 (2001) (Scalia, J., dissenting).

4 *See id.* at 93 (Scalia, J., dissenting) ("[I]t is not even arguable that the testing of urine that has been lawfully obtained is a Fourth Amendment search.").

5 *See* discussion *infra* Part II.

6 *See Ferguson*, 532 U.S. at 84.

7 *See* discussion *infra* Part II.

on conversations, or acquiring data from a third party. "Use" means any action taken in connection with the collected items or information. This includes testing a urine sample, running an algorithm on a data set, sharing collected information with another department or prosecutor, or simply retaining evidence for a period of time.

Law enforcement officers' ability to make use of the evidence they collect has always had practical and scientific boundaries, but those boundaries have dramatically expanded in recent years.[8] As officers make dramatic technological gains in their ability to surveil, analyze, and store information about suspects and potential suspects, the Supreme Court will feel bound to reign them in. For decades, the Court has been able to exercise fine-grain control over collection: officers may search suspects incident to arrest, looking inside containers on their person as small as a cigarette pack,[9] but they may not look at the contents of a suspect's cell phone.[10] Warrantless breath tests incident to arrests for drunk driving are permissible, but warrantless blood tests are not.[11] Officers may use a hidden beeper to track a suspect without a warrant,[12] but if the beeper enters a suspect's home, then the officers must get a warrant.[13] If the Court exerted this level of control over how law enforcement may *use* the material they collect, the Court would effectively double the size of its Fourth Amendment toolbox. The Court will be increasingly drawn towards imposing use restrictions as advancing technologies increasingly undercut the power of their current collection-oriented doctrines.

Part I of this Article explains the traditional approach to searches and seizures under the Fourth Amendment. The Court first looks to see if an

---

8 *See, e.g.*, Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot*, N.Y. TIMES (May 23, 2016), http://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html?&moduleDetail=section-news-3&action=click&contentCollection=U.S.&region=Footer&module=MoreInSection&version=WhatsNext&contentID=WhatsNext&pgty (describing an algorithm that predicts who will be involved in violent crimes); *Is Predictive Policing the Law-Enforcement Tactic of the Future?*, WALL ST. J. (Apr. 24, 2016), http://www.wsj.com/articles/is-predictive-policing-the-law-enforcement-tactic-of-the-future-1461550190 (debating the use of policing algorithms that predict where crimes will occur); Rocco Parascandola & Tina Moore, *Nowhere to Hide from NYPD's Computer System*, N.Y. DAILY NEWS (Aug. 8, 2012), http://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135 (describing New York City's Domain Awareness System); Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST (Feb. 5, 2014), https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html (describing the use of aerial cameras to surveil streets).

9 *See* United States v. Robinson, 414 U.S. 218, 223–24 (1973).

10 *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014); Charles E. MacLean, *But, Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. COURTS L. REV. 41, 43 (2012) (explaining why cell phones should be treated differently from other objects found incident to arrest).

11 *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2184 (2016).

12 *See* United States v. Knotts, 460 U.S. 276, 285 (1983) (Brennan, J., concurring).

13 *See* United States v. Karo, 468 U.S. 705, 715 (1984).

instance of law enforcement collection constitutes a "search or seizure" under the Fourth Amendment.[14] If so, the Court determines if the search or seizure is "reasonable."[15] If the collection is not a search or seizure, or alternatively, if the search or seizure is reasonable, then the Court's analysis ends.[16] There is no back-end analysis of law enforcement's use of the collected material.

Part II of this Article reveals how the Court has deviated from this traditional approach. In multiple cases, the use of collected material, rather than its collection, drove the Court's holdings.[17] In these cases, the Court purported to hold only that a given collection was or was not constitutional, but in fact, the Court's assessment of the government's actual or planned use of the collected material drives its holdings.

In Part III, this Article shows why the Court is likely to more openly impose use restrictions in the future. Previously, when the Court faced a new technology, it was usually a new collection instrument such as a wiretap, a drug-sniffing dog, or heat vision goggles.[18] The Court could readily pursue a course of equilibrium adjustment by imposing restrictions on how the police collect evidence. By contrast, the Court may soon face new technologies that are simply new uses of old collection methods, such as using facial recognition technology to track a suspect through a system of existing traffic cameras or using algorithms to analyze all of a suspect's social connections to determine his likelihood of becoming involved with violent crime.

Part IV of this Article explains how the Court should restrict novel and surprising uses under a new, two-track approach. In situations where the Court is able to prohibit the antecedent collection, it should restrict a given use by finding that the use makes the antecedent collection an unreasonable search. In situations where the Court is unable (for practical or doctrinal reasons) to prohibit the antecedent search, it should restrict the use directly by calling it a "search" in its own right that can be analyzed for reasonableness under the Fourth Amendment. Which approach the Court takes will hinge on whether it can realistically prohibit the antecedent collection. This two-track approach is grounded both in the Supreme Court's precedents and in the original purpose of the Fourth Amendment.

---

14 *See, e.g.*, United States v. Jones, 565 U.S. 400, 404–06 (2012) (describing the Fourth Amendment test); Kyllo v. United States, 533 U.S. 27, 31 (2001) (describing the "antecedent question whether or not a Fourth Amendment 'search' has occurred").

15 *See* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).

16 *See id.*

17 *See* Maryland v. King, 133 S. Ct. 1958, 1977 (2013); NASA v. Nelson, 562 U.S. 134, 156 (2011); Ferguson v. City of Charleston, 532 U.S. 67, 70 (2001); Nixon v. Admin. of Gen. Servs., 433 U.S. 425, 458 (1977); Whalen v. Roe, 429 U.S. 589, 591 (1977).

18 *See Kyllo*, 533 U.S. at 29; United States v. Place, 462 U.S. 696, 697–98 (1983); Katz v. United States, 389 U.S. 347, 348 (1967).

I. COLLECTION RESTRICTIONS UNDER THE TRADITIONAL FOURTH AMENDMENT APPROACH

This Part explains the traditional approach to the Fourth Amendment, wherein courts only impose collection restrictions. It then discusses a subset of Fourth Amendment cases governed by the "special needs" doctrine. These cases differ from most Fourth Amendment cases in that a search or seizure is permitted without a warrant, even without individualized suspicion in many cases.[19] This Part concludes by explaining how the Court's special needs cases pave the way for use restrictions.

A. *The Traditional Fourth Amendment Approach*

Katz v. United States[20] is the foundational case of modern Fourth Amendment jurisprudence. In *Katz*, FBI agents targeted a suspected bookie named Charles Katz.[21] The FBI agents knew Katz regularly used a specific public telephone booth, so they attached a recording device to the outside of the phone booth.[22] The agents did not have a warrant to use the recording device.[23] Using the device, the FBI agents were able to record Katz communicating wagers around the country.[24] These recordings were used against Katz in court, and he was convicted.[25] Katz challenged the use of the recordings at his trial.[26]

The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[27]

Arguably, the most logical part of the amendment to focus on is the enumerated list of "persons, houses, papers, and effects."[28] These are at least four things the Fourth Amendment protects, and the Court could have debated whether a phone conversation fit into the list. However, in *Katz*, the Supreme Court focused on the word "unreasonable."[29] More specifically, Justice

---

19 *See* discussion *infra* Part I.B.
20 389 U.S. 347 (1967).
21 *Id.* at 348.
22 *Id.* at 354 n.14.
23 *Id.*
24 *Id.* at 348.
25 *Id.*
26 *Katz*, 389 U.S. at 348–49.
27 U.S. CONST. amend. IV.
28 *Id.*
29 *Katz*, 389 U.S. at 354.

Harlan did so in his concurrence, which became the most oft-cited part of the opinion.[30] Justice Harlan explained:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[31]

The Supreme Court has fully adopted Justice Harlan's reasoning.[32] In recent cases, it has summarized Harlan's concurrence as the simple rule: "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[33] The Court often combines the two prongs to speak in terms of a party having a "reasonable expectation of privacy."[34]

Once the Court determines that a reasonable expectation of privacy was violated, and therefore a search has occurred, the Court asks if the search itself was "unreasonable."[35] If the search was "unreasonable," then the Fourth Amendment prohibits it.[36] Generally, for a search to be "reasonable," a warrant is required.[37] However, there are a number of exceptions to the warrant requirement. These include searches incident to arrest,[38] automobile searches,[39] and searches that fall under the "special needs" doctrine,[40] all of which may be performed without a warrant. Because "the Fourth Amendment does not specify when a search warrant must be obtained,"[41] many Supreme Court cases find that a search has occurred and then proceed to analyze whether the search was reasonable, despite the lack of a warrant.[42]

Two examples may be helpful to illustrate the Court's traditional, collection-centered approach. In *California v. Greenwood*,[43] the Court held that the police officers' actions were not a "search," so their actions were

---

30 *See* Kyllo v. United States, 533 U.S. 27, 33 (2001) (describing the concurrence as "oft-quoted").

31 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

32 *See, e.g.*, United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 33.

33 *Kyllo*, 533 U.S. at 33.

34 *See, e.g.*, City of Los Angeles v. Patel, 135 S. Ct. 2443, 2448 (2015); City of Ontario v. Quon, 560 U.S. 746, 760 (2010); Dow Chem. Co. v. United States, 476 U.S. 227, 235 (1986).

35 *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).

36 *Id.*

37 Kentucky v. King, 563 U.S. 452, 459 (2011).

38 *See* Weeks v. United States, 232 U.S. 383, 392 (1914) (recognizing in dictum that searches incident to arrest were always permissible under English and American law), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961).

39 *See* Carroll v. United States, 267 U.S. 132, 156 (1925).

40 *See T.L.O.*, 469 U.S. at 351 (Blackmun, J., concurring).

41 *King*, 563 U.S. at 459.

42 *See, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 618–19 (1989); *T.L.O.*, 469 U.S. at 337.

43 486 U.S. 35 (1988).

permissible under the Fourth Amendment.[44] An investigator received a tip that Billy Greenwood might be involved in narcotics trafficking.[45] The investigator asked Greenwood's trash collector to give her Greenwood's trash bags so she could look for evidence of narcotics.[46] She did not have a warrant to search the trash bags.[47] The investigator found evidence "indicative of narcotics use" and was able to obtain a warrant to search Greenwood's home based on what she found in his trash.[48] A search of Greenwood's home turned up "quantities of cocaine and hashish," leading to his arrest.[49]

The issue before the Supreme Court was whether the Fourth Amendment prohibited officers from warrantlessly seizing and searching a person's trash that was left outside for pickup.[50] The Court held that it did not.[51] The Court's analysis was entirely collection-oriented. The Court opened with the *Katz* question of whether Greenwood had a reasonable expectation of privacy in his trash.[52] The Court held that any expectation of privacy was not objectively reasonable because trash bags left outside were "readily accessible to animals, children, scavengers, snoops, and other members of the public."[53] Moreover, Greenwood clearly anticipated that a third party (the garbage man) would collect his trash, thereby eliminating any reasonable expectation of privacy in his trash.[54] Greenwood's expectations were framed in terms of who he reasonably expected to view his trash, not what he expected a third party to use his trash for.[55]

The *Katz* inquiry was the beginning and the end of the Court's analysis. Once it determined that the collection was not a "search," the Court did not explore how the investigator was permitted or not permitted to use Greenwood's trash.[56] The analysis did not necessarily have to end there, since a person's trash may reveal many private facts about them. A person's trash could contain pill bottles, a pregnancy test, private letters, evidence of sexual activity, or sensitive documents related to a person's job. The Court could have been concerned about the state retaining or disseminating private material found in the trash. However, the law enforcement officers gave the Court no reason to worry about their intended uses for Greenwood's trash. They found evidence of drugs, used that evidence to obtain a warrant to search his

---

44 *Id.* at 37.

45 *Id.*

46 *Id.*

47 *Id.*

48 *See id.* at 37–38.

49 *Greenwood*, 486 U.S. at 38.

50 *Id.* at 37.

51 *Id.*

52 *Id.* at 39–41.

53 *Id.* at 39–40 (footnotes omitted).

54 *Id.* at 40–41.

55 *Greenwood*, 486 U.S. at 41.

56 *See id.* at 55–56 (Brennan, J., dissenting) (noting that the Court's opinion allows arbitrary monitoring).

house for drugs, and arrested him for possessing drugs.[57] Because the use of the evidence was immediate and unsurprising, the Court could comfortably be in control of the consequences of the investigators' trash rummaging simply by deciding whether to permit the collection.

United States v. Robinson[58] is an example of a case where the Court found a police officer's actions were a "search" but held that the search was reasonable despite lacking a warrant.[59] An officer arrested Willie Robinson for operating a vehicle after his permit had been revoked.[60] The officer then searched Mr. Robinson incident to the arrest and found a crumpled up cigarette pack.[61] The officer looked inside the cigarette pack and found fourteen capsules of heroin.[62] Mr. Robinson was convicted for heroin possession.[63] He challenged the search on Fourth Amendment grounds.[64]

The Court began by noting "[i]t is well settled that a search incident to a lawful arrest is a traditional exception to the warrant requirement of the Fourth Amendment."[65] Since the officer thoroughly patted Mr. Robinson down and looked in his pockets, the Court did not bother explaining why this personal physical intrusion was clearly a "search" under the Fourth Amendment.[66] The Court instead went through the historical background of the warrant exception for searches incident to arrest and ultimately determined that "[a] custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification."[67] A "full search" of Mr. Robinson was permitted under the Fourth Amendment, including a search of the inside of his cigarette pack.[68]

Once again, the moment of collection was the only moment that mattered for the Court's analysis. The Court highlighted how once a search was permitted, the consequences were naturally permitted as well:

> [I]t is of no moment that [Officer] Jenks did not indicate any subjective fear of the respondent or that he did not himself suspect that respondent was armed. Having in the course of a lawful search come upon the crumpled package of cigarettes, he was entitled to inspect it; and when his inspection revealed the heroin capsules, he was entitled to seize them as 'fruits, instrumentalities, or contraband' probative of criminal conduct.[69]

---

57 *Id.* at 37–38.
58 414 U.S. 218 (1973).
59 *Id.* at 224, 235.
60 *Id.* at 220–21.
61 *Id.* at 221–23.
62 *Id.* at 223.
63 *Id.* at 219.
64 *Robinson*, 414 U.S. at 220.
65 *Id.* at 224.
66 *See id.* at 223–24.
67 *Id.* at 235.
68 *See id.*
69 *Id.* at 236 (quoting Harris v. United States, 331 U.S. 145, 154–55 (1947)).

The Court did not pause to analyze the officer's motives or his intended uses for anything he found.[70] The officer's ability to collect evidence from Mr. Robinson was the only relevant factor in the analysis.[71]

Greenwood and *Robinson* demonstrate the Court's traditional approach to Fourth Amendment cases. First, determine whether a given governmental action is a search (based on the *Katz* reasonable expectation test).[72] And second, if the action is a search, decide whether the search was reasonable despite lacking a warrant.[73] Both stages traditionally focus solely on collection, not on the intended uses for the uncovered material. Next, this Article explains the "special needs" exception to the warrant requirement, which focuses on the purposes of a search.

B. *"Special Needs" Cases*

Special needs cases significantly differ from traditional Fourth Amendment cases. They are particularly relevant to this Article because, unlike most Fourth Amendment cases, they openly consider how collected material was used.[74] The special needs cases all involve "searches," and the use of the material speaks to whether the search at issue was reasonable.[75]

A "special need" is defined as a need other than "the normal need for law enforcement" that leads to a search.[76] The Justices have differed on whether this need must have a certain degree of demonstrated importance or whether simply falling outside the police's normal crime-fighting mission is sufficient.[77] When handling a special needs case, the Court does not engage in the typical analysis described in the previous section. The probable cause

---

70 *Cf. Robinson*, 414 U.S. at 239 (Marshall, J., dissenting) (explaining that the majority's opinion establishes the authority to conduct a full search, even if a particular case lacks other reasons for performing a search incident to arrest).

71 *See id.* at 235.

72 *See* Russell W. Galloway, Jr., *Basic Fourth Amendment Analysis*, 32 SANTA CLARA L. REV. 737, 742–43 (1992).

73 *See id.* at 767.

74 *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (holding that the hospital's search program was unreasonable because there was a privacy expectation that the collected urine results from pregnant women at the hospital would not be shared with nonmedical personnel).

75 *See id.* at 86 (holding that because the use of the urine results violated an expectation of patient privacy, the search program was unreasonable and in violation of the Fourth Amendment); discussion *infra* Parts II.A & II.B (discussing how the use of collected material influences Fourth Amendment court decisions).

76 Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989) (citation omitted).

77 *Compare* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 684 (1989) (Scalia, J., dissenting) (stating that the Court's precedents have required a "special need" to include "well-known or well-demonstrated evils *in that field*, with well-known or well-demonstrated consequences"), *with* Chandler v. Miller, 520 U.S. 305, 325 (1997) (Rehnquist, C.J., dissenting) ("Under our precedents, if there was a proper governmental purpose other than law enforcement, there was a 'special need.'").

requirement present in the text of the Fourth Amendment can be ignored.[78] Furthermore, even an individualized suspicion of wrongdoing is not necessarily required.[79]

Once the Court determines there is a "special need" in a given case, the Court balances the individual's privacy interest against the government's needs.[80] This balance often includes a petitioner's decreased expectation of privacy due to his particular circumstances, the overall intrusiveness of the search, and the strength of the government's need.[81] The exact factors that are balanced vary to some degree by case.[82] Regardless of the precise factors used, the balance usually comes out in the government's favor.[83]

In *Vernonia School District 47J v. Acton*,[84] a school district had implemented a program for drug testing the urine of student athletes.[85] The Court held that the warrantless and suspicionless urinalysis program was constitutional.[86] The Court analyzed a number of factors to make this determination. First, it examined "the nature of the privacy interest upon which the search here at issue intrudes."[87] The student athletes were found to have significantly reduced expectations of privacy because they were children committed to the temporary custody of the state and student athletes "subject themselves to a degree of regulation even higher than that imposed on students generally."[88]

Next, the Court analyzed "the character of the intrusion that is complained of."[89] The Court considered the physical circumstances under which

---

78 *See* New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) ("Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers.").

79 *See Von Raab*, 489 U.S. at 668 ("Our precedents have settled that, in certain limited circumstances, the Government's need to discover such latent or hidden conditions, or to prevent their development, is sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion.").

80 *See, e.g.*, *T.L.O.*, 469 U.S. at 340.

81 *See, e.g.*, *Skinner*, 489 U.S. at 622–23.

82 The Court has developed specific tests for specific contexts in some cases. For instance, in cases where the state actor performing a search is a government employer, the Court first establishes whether there was a "'noninvestigatory, work-related purpose[e]'" for the search and then examines if the search was "'justified at its inception' and if 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of' the circumstances giving rise to the search." City of Ontario v. Quon, 560 U.S. 746, 761 (alteration in original) (quoting O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987), *aff'd*, 146 F.3d 1149 (9th Cir. 1998)).

83 *See Skinner*, 489 U.S. at 639 (Marshall, J., dissenting) ("Tellingly, each time the Court has found that 'special needs' counseled ignoring the literal requirements of the Fourth Amendment for such full-scale searches in favor of a formless and unguided 'reasonableness' balancing inquiry, it has concluded that the search in question satisfied that test.").

84 515 U.S. 646 (1995).

85 *Id.* at 650.

86 *Id.* at 665.

87 *Id.* at 654.

88 *Id.* at 656–57.

89 *Id.* at 658.

the students had to produce the urine sample (in an enclosed stall, with a monitor listening), what information the urine tests revealed about the students, who received the test results, whether the search was undertaken for punitive or nonpunitive purposes, and the effect of requiring students to reveal what medications they were taking before the test.[90] Given these elements, the Court found the privacy invasion was "not significant."[91]

The last factor the Court considered was "the nature and immediacy of the governmental concern at issue here, and the efficacy of this means for meeting it."[92] The Court found the drug use in the district created an immediate and important problem, and one that was effectively addressed by the testing program.[93] On balance, the Court found that the above factors weighed in favor of the program being reasonable and therefore not violative of the Fourth Amendment.[94]

Vernonia placed great emphasis on the school district's purpose and role.[95] The Court identified "[t]he most significant element in this case" as the fact that the program was "undertaken in furtherance of the government's responsibilities, under a public school system, as guardian and tutor of children entrusted to its care."[96] Rather than the usual "reasonable expectation" standard present in *Katz*, the Court's analysis suggested a "reasonable guardian" standard may be present in special needs cases set in schools.[97] The Court stated that "when the government acts as guardian and tutor the relevant question is whether the search is one that a reasonable guardian and tutor might undertake."[98]

Special needs cases speak explicitly about "purpose," which is often a critical element in the analysis, as it was in *Vernonia*.[99] Special needs cases are not "special" if there is not a non–law enforcement purpose primarily motivating the search.[100] However, this does not mean that the results of special needs searches cannot be *used* in criminal proceedings. They can. The "purpose" of a sobriety checkpoint is to prevent drunk driving,[101] but drunk drivers who pass through a checkpoint can be prosecuted.[102] The prosecution is a permissible "use" of the breathalyzer results. While the Court has a track record in special needs cases of explicitly deciding cases based on the

---

90 *Vernonia*, 515 U.S. at 658–60.

91 *Id.* at 660.

92 *Id.*

93 *Id.* at 660–64.

94 *Id.* at 664–65.

95 *Id.* at 650.

96 *Vernonia*, 515 U.S. at 665.

97 *Id.*

98 *Id.*

99 *See* City of Ontario v. Quon, 560 U.S. 746, 764 (2010) ("Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable.").

100 Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989).

101 *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

102 *See id.* at 448.

"purpose" of a search program, it does not have a comparable record of explicitly deciding cases based on how a search program *uses* the evidence it uncovers.[103]

Nevertheless, many special needs cases do consider the use of the collected material.[104] This will be explored further in the following Part; here it is sufficient to note that the *Vernonia* Court considered aspects of how the drug tests were used, such as who received the test results and what the consequences of failing a drug test were.[105] The Court highlighted that the results were released only to those "who ha[d] a need to know."[106] Additionally, the Court observed that the results were "not turned over to law enforcement authorities or used for any internal disciplinary function."[107] These facts weighed in favor of the Court's finding that the drug tests were not overly invasive of the students' privacy interests.[108] This analysis stands in stark contrast to *Katz*, *Greenwood*, and *Robinson*, where there was no consideration of what sensitive information might be revealed by the government's wiretapping or trash rummaging.[109] Those cases did not mention any limitations on who could view the evidence.[110] Nor did they discuss the consequences for the incriminating evidence—the legal consequences were obvious, and did not worry the Court.[111]

It makes sense that special needs cases consider both the government's purpose behind a search, and its subsequent uses for the material it collects, while most traditional Fourth Amendment cases consider neither purpose nor use. Special needs cases must pay attention to the purpose behind a search: it is the presence of a need besides "the normal need for law enforcement" that makes the case a "special needs" case.[112] Why a program's purpose should trigger a different constitutional standard is a valid question, and one the Court has not been entirely upfront about answering.[113] It appears to be a combination of (1) the fact that requiring schoolteachers and similar

---

103 *Compare Vernonia*, 515 U.S. at 650 (holding the search program was reasonable because the expressed purpose was to protect the health and safety of student athletes), *with* Ferguson v. City of Charleston, 532 U.S. 67, 83–84 (2001) (holding that because the "primary purpose" of the search program "was to use the threat of arrest and prosecution in order to force women into treatment," and because law enforcement was extensively involved at every stage of the program, the search was unreasonable).

104 *See* discussion *infra* Parts II.A & II.B.

105 *Vernonia*, 515 U.S. at 658.

106 *Id.*

107 *Id.*

108 *Id.* at 660.

109 *See* discussion *supra* Part I.A (discussing the traditional analysis of Fourth Amendment cases).

110 *See* discussion *supra* Part I.A.

111 *See* discussion *supra* Part I.A.

112 Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989).

113 *But see, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 46–47 (2000) ("While we recognize the challenges inherent in a purpose inquiry, courts routinely engage in this enterprise in many areas of constitutional jurisprudence as a means of sifting abusive governmental conduct from that which is lawful.").

government agents to obtain warrants simply seems impracticable[114] and (2) the instinct that if traditional law enforcement motives are not in play, individuals will be relatively safe from criminal prosecution, so a lesser degree of constitutional protection is appropriate.[115]

The second difference between traditional Fourth Amendment cases and special needs cases is whether the Court generally considers the use of collected material. There is usually little reason to analyze how a law enforcement officer might seek to use uncovered evidence; it is obvious he will try to use it in a criminal proceeding.[116] New technologies open up the possibility for more troubling uses, such as the creation of comprehensive nationwide biometric databases, but historically, the Court has been comfortable with how law enforcement uses the material it finds.[117] It is much less obvious what other state actors will do with the material they collect. The school district in *Vernonia* chose not to punish students who tested positive (assuming they chose the drug counseling option),[118] but it is easy to imagine another school district punishing the students in school, or even turning over the evidence to law enforcement. Therefore, in a balance between the government's interest and the individual's interest, it seems logical on both ends to determine what exactly the collected material is being used for. The intended use determines how great the privacy invasion is for the individual, and it speaks to the nature of the government's interest.

Special needs cases naturally lead the Court to consider use restrictions. Special needs cases typically involve large-scale search programs, where searches are conducted without probable cause or even individualized suspicion. Examples include the above-described drug tests for student athletes,[119] drug tests for United States Customs Service employees,[120] and background check questionnaires for federal contractors.[121] A more traditional search like the cigarette pack inspection in *Robinson* affects only one person whose specific situation the Court can carefully consider.[122] Other arrestees will of course be affected by the holding in *Robinson*. But if they feel their searches

---

114 *See Skinner*, 489 U.S. at 619 (stating that special needs cases "make the warrant and probable-cause requirement impracticable" (citation omitted)); New Jersey v. T.L.O., 469 U.S. 325, 340 (1985) (finding that requiring teachers to obtain warrants "would unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools").

115 *See Skinner*, 489 U.S. at 651 (Marshall, J., dissenting) (expressing frustration that the majority dismisses his concern that positive drug tests will be turned over to the authorities, because the majority found that there was no evidence the program "was intended to be, or actually has been, so used"). Justice Marshall noted that there were no restrictions in place to prevent positive drug tests from being turned over to the authorities.

116 *See, e.g.*, California v. Greenwood, 486 U.S. 35, 37–38 (1988) (showing that a police officer collected evidence of narcotic usage from defendant's garbage to acquire a warrant).

117 *See* discussion *infra* Part II.

118 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 651 (1995).

119 *Id.* at 650.

120 *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 660–61 (1989).

121 *See* NASA v. Nelson, 562 U.S. 134, 140–41 (2011).

122 United States v. Robinson, 414 U.S. 218, 223 (1973).

crossed the line drawn in *Robinson*, they can separately challenge their own searches.[123] The Court can then closely consider the circumstances of the new search and draw a new line if necessary.[124] Justice Scalia hated the repeated line drawing required by traditional Fourth Amendment cases, complaining that each case merely answered the constitutional question in "variation 3,542."[125]

However, this line drawing makes for an extraordinary level of control over how material may be collected by government agents. This level of control is notably absent in most special needs cases.[126] The Court often rules on the constitutionality of programs that affect hundreds, if not thousands, of people, and it has to decide if these searches are permissible all at once.[127] Granted, the searches should be more or less comparable, but given the large numbers involved, and the lack of any strict probable cause or individualized suspicion requirements,[128] the Court is unlikely to be sanguine about non–law enforcement actors collecting sensitive information for any and all uses. Rather, the Court will want to compensate for the control it loses when it gives up the probable cause and individualized suspicion standards that are simply a poor fit for special needs cases.

This is not to suggest the Court is wrong to use a different standard for special needs cases. It is hard to imagine training all school teachers on probable cause or running any type of randomized drug test program if individualized suspicion is required. But as the Court has limited its power to regulate collection in special needs cases, it is natural for the Court to seek other ways to prevent unreasonable searches and seizures. The loose balancing test used in special needs cases provides the Court with the perfect opening to consider an element not normally considered under a traditional Fourth Amendment analysis: use.

II. USE RESTRICTIONS UNDER THE FOURTH AMENDMENT

This Part analyzes Supreme Court cases where the use of lawfully collected material has driven the Court's decisions. The first case is the 2001 case *Ferguson v. City of Charleston*,[129] where the Court prohibited a specific use under the Fourth Amendment, though the Court purported to merely

---

123 *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2481 (2014) (challenging the search of a cell phone incident to arrest).

124 *Id.* at 2485 (holding that cell phones may not be searched incident to arrest).

125 Interview by Susan Swain with Antonin Scalia, Assoc. Justice of the U.S. Supreme Court, in D.C. (June 19, 2009), https://www.c-span.org/video/?286079-1/supreme-court-justice-scalia.

126 *See generally* New Jersey v. T.L.O., 469 U.S. 325, 337–41 (1985).

127 *See, e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451 (1990) (ruling on a program that searched for drunk drivers at checkpoints).

128 *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989); *T.L.O.*, 469 U.S. at 352–53 (Blackmun, J., concurring).

129 532 U.S. 67 (2001).

prohibit collection.[130] The second case is *Maryland v. King*,[131] where the use of collected DNA samples was completely elided by the majority's decision but was the focal point of an ardent dissent from four justices.[132] Lastly, this Part examines cases that address an individual's right to control dissemination of his lawfully collected personal information. All together, these cases demonstrate that the use of lawfully collected material has been relevant to the Court's Fourth Amendment case law for some time.[133] Moreover, the case law would be much clearer if the Court openly addressed its desire for use restrictions.

A. *Ferguson v. City of Charleston*

In 1988, the staff at the Medical University of South Carolina ("MUSC") became concerned about an apparent increase in the number of "crack babies"—infants seriously harmed by their mother's cocaine use.[134] MUSC is a state hospital, so its staff are government actors subject to the Fourth Amendment.[135] The hospital implemented a program in which the urine of pregnant women who met certain criteria were tested for cocaine.[136] If a woman tested positive for cocaine, she was referred to the county substance abuse commission for counseling and treatment.[137] However, this program did not appear to reduce the incidence of cocaine use among pregnant women at MUSC.[138]

A few months later, a nurse who was the case manager for the obstetrics department heard a news report about police arresting pregnant women who used cocaine, on the theory that they were committing child abuse.[139] She spoke to MUSC's general counsel about the report, and he contacted the city prosecutor.[140] The prosecutor formed a task force with MUSC staff that developed a policy wherein pregnant women's urine would be tested if the women met certain criteria.[141] The criteria for deciding which women would be tested were largely the same as those utilized before the task force was created.[142] Under the new policy, if a woman tested positive for cocaine while

---

130 *Id.* at 83–84.
131 569 U.S. 435 (2013).
132 *Id.* at 470–76.
133 *See id.* at 448–49; *Ferguson*, 532 U.S. at 77–78.
134 *Id.* at 70.
135 *Id.* at 76.
136 *Id.* at 70.
137 *Id.*
138 *Id.*
139 *Ferguson*, 532 U.S. at 70.
140 *Id.* at 70–71.
141 *Id.* at 71.
142 The petition for certiorari listed the criteria for testing as follows:
1. No prenatal care 2. Late prenatal care after 24 weeks gestation 3. Incomplete prenatal care 4. Abruptio placentae 5. Intrauterine fetal death 6. Preterm labor "of no obvious cause" 7.

pregnant, she would still be referred to a substance abuse counselor, but she would do so under threat that if she missed an appointment with her counselor or tested positive again, the police would be notified and she would be arrested.[143]

Ten women arrested pursuant to the policy brought various challenges.[144] The Supreme Court granted certiorari on the question of whether the special needs doctrine applied to the women's cases.[145] For the purposes of the opinion, the Court assumed that the women did not consent to a search.[146]

The Court held that this was not a special needs case.[147] The Court acknowledged that "the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs," but nevertheless, "the immediate objective of the searches was to generate evidence *for law enforcement purposes* in order to reach that goal."[148] The Court specified that searches could not be immunized by looking to the program's "ultimate, rather than immediate, purpose."[149] A "benign" motive could not justify departing from the traditional Fourth Amendment standards, "given the pervasive involvement of law enforcement with the development and application of the MUSC policy."[150] The Court was clearly concerned about the "substantial" invasion of privacy when a woman's diagnostic tests were "shared with nonmedical personnel without her consent."[151] Therefore, the searches were forbidden under the "Fourth Amendment's general prohibition against nonconsensual, warrantless, and suspicionless searches."[152]

Justice Scalia, joined by Chief Justice Rehnquist and Justice Thomas, dissented.[153] Justice Scalia highlighted an issue the majority elided: what exactly was the search at issue?[154] The complained-of behavior could be broken

---

IUGR [intrauterine growth retardation] "of no obvious cause" 8. Previously known drug or alcohol abuse 9. Unexplained congenital anomalies.

Id. at 71 n.4. The Fourth Circuit quoted the nurse as saying the initial criteria for testing a pregnant woman's urine were "no prenatal care, late prenatal care, abruptio placentae, intrauterine fetal death, preterm labor, and there was one other one that was supposed to be screened prenatally or at delivery." Ferguson v. City of Charleston, 308 F.3d 380, 408 (4th Cir. 2002).

143 *Ferguson*, 532 U.S. at 72. The new policy at first mandated that a positive test would immediately result in arrest, but this was soon modified to give the woman a second chance. *Id.* at 72 n.5.

144 *Id.* at 73.

145 *Id.* at 76.

146 *Id.* The Court remanded the case to the Fourth Circuit to decide the consent issue. *Id.*

147 *Ferguson*, 532 U.S. at 86.

148 *Id.* at 82–83 (footnote omitted).

149 *Id.* at 84.

150 *Id.* at 85.

151 *Id.* at 78 ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

152 *Id.* at 86.

153 *Ferguson*, 532 U.S. at 91 (Scalia, J., dissenting). Justice Kennedy wrote an opinion that solely concurred in the judgment. *Id.* at 86 (Kennedy, J., concurring in judgment).

154 *Id.* at 92 (Scalia, J., dissenting).

into three parts: the collection of the urine, the testing of the urine, and the sharing of the test results with the police.[155] Justice Scalia stated that the hospital's sharing the test results with the police was "obviously not a search."[156] Additionally, "it is not even arguable that the testing of urine that has been lawfully obtained is a Fourth Amendment search."[157] In Justice Scalia's view, "[t]here is only one act that could conceivably be regarded as a search of petitioners in the present case: the *taking* of the urine sample."[158] Justice Scalia concluded that the collection was consented to, as there was no evidence of coercion.[159] Therefore, there was no "search" for the Court to analyze.[160]

Justice Scalia went on to argue that even if there were a search, the special needs doctrine would apply to validate the search.[161] The purpose of the program was plainly to provide health benefits to expectant mothers and their children, as reflected by the fact that MUSC began drug testing pregnant women months before law enforcement officials were brought in.[162] Justice Scalia argued "[t]hat the *addition* of a law-enforcement-related purpose *to* a legitimate medical purpose" could not possibly make the special needs doctrine inapplicable.[163] Moreover, even though the Court's ruling ostensibly invalidated all aspects of the hospital's policy, he asked if the Court could "really believe (or even *hope*) that, once invalidation of the program challenged here has been decreed, drug testing will cease?"[164]

The answer had to be "no." No party challenged the drug tests prior to law enforcement's involvement,[165] and it is unlikely that the Court meant to invalidate any urine tests solely used to prevent the birth of irreparably harmed babies. The Court repeatedly emphasized in its majority opinion that the hospital's policy did not fall under the special needs doctrine because (1) the "primary purpose" of the policy was to threaten the women with arrest and prosecution, and (2) law enforcement officials were extensively involved at every stage of the policy's development and implementation.[166] The

---

155 *Id.*

156 *Id.*

157 *Id.* at 93.

158 *Ferguson*, 532 U.S. at 92 (Scalia, J., dissenting).

159 *Id.* at 93.

160 *See id.*

161 *Id.* at 98.

162 *Id.* at 99.

163 *Id.* at 100.

164 *Ferguson*, 532 U.S. at 100 (Scalia, J., dissenting).

165 Ferguson v. City of Charleston, 308 F.3d 380, 408 (4th Cir. 2002) (Niemeyer, J., concurring in part and dissenting in part).

166 *Ferguson*, 532 U.S. at 84. The majority emphasizes these same two points just two paragraphs later:

> Such a [benign] motive, however, cannot justify a departure from Fourth Amendment protections, given the pervasive involvement of law enforcement with the development and application of the MUSC policy. The stark and unique fact that characterizes this case is that Policy M–7 was designed to obtain evidence of criminal conduct by the tested patients that would be turned over to the police and that could be admissible in subsequent criminal prosecutions.

majority opinion provided no reason to prohibit the urine tests in the absence of law enforcement. However, it did not single out the sharing of the test results as an unconstitutional search by itself.[167] Instead, it implicitly allowed the collection and testing program to continue, so long as the results were not shared with law enforcement.[168] Therefore, despite not explicitly announcing it, the *Ferguson* Court created a use restriction under the Fourth Amendment.

B. *Maryland v. King*

This Article next explores a 5-4 decision where the Court did not impose a use restriction, but a questionable use was at the heart of the fight between the majority and the dissent.

In *Maryland v. King*, the Court examined the Maryland DNA Collection Act.[169] The Act authorizes law enforcement officers to collect DNA samples from "an individual who is charged with . . . a crime of violence or an attempt to commit a crime of violence; or . . . burglary or an attempt to commit burglary."[170] DNA samples may not be placed in a database until the individual is arraigned.[171] If a court finds that the relevant charges are not supported by probable cause, or if the individual is later acquitted, the DNA sample is destroyed.[172] Moreover, the only information that may be stored about the DNA sample is genetic information that identifies the individual through so-called "junk DNA," which does not reveal any genetic predispositions but is sufficiently unique to be extremely useful for identifying an individual.[173]

In 2009, Alonzo King was charged with assault for menacing people with a shotgun.[174] His DNA was taken with a quick cheek swab.[175] After some time, his DNA was matched to a DNA sample from an unsolved rape case.[176] He moved to suppress the DNA match on the ground that the Act violated

---

Id. at 85–86.

167 The Court did not separately analyze the collection, testing, and sharing of the test results but instead referred generally to invalidating the entire "policy." *See id.* at 81 (describing its "review of the M-7 policy"). It would be difficult to characterize sharing test results as a "search." *See Search*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/search (last visited Feb. 6, 2018) (defining "search" as an effort "to look into or over carefully or thoroughly in an effort to find or discover something").

168 *See Ferguson*, 532 U.S. at 81–84.

169 Maryland v. King, 569 U.S. 435, 441 (2013).

170 *Id.* at 443 (quoting MD. CODE ANN., PUB. SAFETY § 2-504(a)(3)(i) (West 2011)).

171 *Id.*

172 *Id.*

173 *Id.* at 442–43, 445.

174 *Id.* at 440.

175 *King*, 569 U.S. at 440.

176 *Id.*

the Fourth Amendment.[177] His motion was defeated, and King was tried for and convicted of the rape.[178]

The Court found that the search under the Act was constitutional.[179] Justice Kennedy's majority opinion was long and not a model of clarity. The Court began by detailing the protections of the Act.[180] The Court then stated that obtaining a DNA sample via a cheek swab is a search.[181] The Court next explained the special needs doctrine and stated that "[t]he instant case [could] be addressed with this background."[182] However, the Court later said the special needs doctrine "d[id] not have a direct bearing on the issues presented in this case," but the special needs cases nevertheless were "in full accord with the result reached here."[183] The special needs doctrine appeared to be triggered by the special need to identify arrestees, but the doctrine purportedly was not directly relevant because "a detainee has a reduced expectation of privacy."[184]

The Court did not explicitly apply the special needs doctrine but stated that "[a]n assessment of reasonableness to determine the lawfulness of requiring this class of arrestees to provide a DNA sample [was] central to the instant case."[185] This "assessment of reasonableness" required the Court to balance "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'"[186] This balancing was later performed with a noticeable similarity to a special needs balancing.[187]

The Court then weighed the government interest in identification, the unique effectiveness of DNA identification, the minimal intrusion of a cheek swab, an arrestee's diminished expectations of privacy, and the extent to which "the processing of respondent's DNA sample" intruded on his privacy.[188] The Court reiterated the many protections under the Act and explained that "[i]f in the future police analyze[d] samples to determine, for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here."[189] The Court did not separately analyze the use of King's DNA to match him to the unsolved rape case.[190]

---

177 *Id.* at 441.
178 *Id.*
179 *Id.* at 465–66.
180 *Id.* at 443–44.
181 *King*, 569 U.S. at 446.
182 *Id.* at 447.
183 *Id.* at 463.
184 *Id.*
185 *Id.* at 448.
186 *Id.* (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
187 *King*, 569 U.S. at 461–64.
188 *Id.* at 461–65.
189 *Id.* at 464–65.
190 *See id.* at 459–65.

Justice Scalia's dissent was joined by Justice Ginsburg, Justice Kagan, and Justice Sotomayor.[191] In a striking contrast to the majority opinion, it was entirely focused on the use of King's DNA to match him to the unsolved rape case.[192] Justice Scalia argued that "[t]he Court's assertion that DNA is being taken, not to solve crimes, but to *identify* those in the State's custody, taxes the credulity of the credulous."[193] The special needs doctrine is applied only where the primary purpose of a search is not law enforcement's ordinary crime-solving purpose.[194] Since King's DNA was taken for the purpose of using it to solve old crimes, there was no "special need" and therefore no excuse for engaging in "the free-form 'reasonableness' inquiry that the Court indulges at length today."[195]

Justice Scalia supported his dissent with several additional facts. There was no uncertainty about who King was from the outset, undercutting the majority's identification justification.[196] King's DNA was not matched to the unsolved rape case until four months after his DNA sample was taken.[197] The database his DNA was placed into could not have identified him; rather, his DNA was placed in a database where it could identify unknown DNA samples.[198] Lastly, the Act itself and the lawmakers involved with it made clear that the Act was a "crime-fighting tool," not an identity-documenting tool.[199]

The dissent also explicitly discussed use. Fingerprints, Justice Scalia argued, are truly taken to identify arrestees, though, he acknowledged, "that process sometimes solves crimes."[200] DNA, however, "is taken to solve crimes (and nothing else)."[201] This difference in use matters when deciding whether there is a "special need" that justifies disregarding the warrant and probable cause requirements of the Fourth Amendment.[202]

In *King*, Justice Scalia and Justice Kennedy took advantage of the manipulability of the special needs doctrine to consider use at two different stages of their analyses. Justice Scalia treated use as determinative of purpose and then focused exclusively on use/purpose in his dissent.[203] Justice Kennedy essentially skipped over the threshold purpose question of the special needs doctrine by asserting that the special needs doctrine "d[id] not have a direct bearing on the issues presented in this case."[204] He instead jumped to

---

191 *Id.* at 466 (Scalia, J., dissenting).

192 *See id.* at 470–74

193 *King*, 569 U.S. at 466 (Scalia, J., dissenting).

194 *Id.* at 468.

195 *Id.* at 468–69 n.1.

196 *Id.* at 470.

197 *Id.* at 472.

198 *Id.* at 473–74.

199 *King*, 569 U.S. at 474–75 (Scalia, J., dissenting) (quoting Jean Marbella, *Supreme Court Will Review Md. DNA Law*, BALT. SUN, Nov. 10, 2012, at A1, A14).

200 *Id.* at 478.

201 *Id.*

202 *See id.* at 480–81.

203 *Id.* at 474–76.

204 *Id.* at 463 (majority opinion).

balancing the government's interest in identification against the individual's privacy interests.[205] When engaging in this balancing, he cited *T.L.O.* and *Vernonia*, two prototypical special needs cases.[206] These citations highlight the special needs reasoning of the case. Yet in lieu of a preliminary discussion of the Act's purpose, Justice Kennedy shored up his identification rationale with an extended discourse on the history of officers taking photographs, fingerprints, and "Bertillon measurements"[207] as part of the normal booking process for arrestees.[208]

In some ways, *King* is a surprising result. In *Ferguson*, the purpose of the policy and the way the collected material was used were at odds.[209] The purpose of the policy (despite the majority's contortions) was to help unborn children and their mothers.[210] The use at issue was sharing drug test results with law enforcement so the police could arrest pregnant women and new mothers.[211] In *King*, the purpose of the Act and the use of the DNA samples were in perfect alignment.[212] The purpose was to solve crimes, and King's DNA was used to solve crimes.[213] Despite this unity, the dissenters were unable to persuade a fifth Justice to join this very straightforward special needs analysis.[214] Why didn't the cleaner legal reasoning win the day?

The answer is that both cases turned on how the Justices felt about the way the collected material was used. As described above, the *Ferguson* Court twisted itself in knots trying to mold the law enforcement involvement and use of the urine samples into the policy's purpose.[215] The Court could not abide the idea of pregnant women giving urine samples to their doctors and then having their urinalysis results turned over to the police so that they might be arrested, often directly after giving birth, still in their hospital gowns.[216] However, in *King*, the Court did not have a problem with the use at issue. Catching a violent rapist is an extremely worthwhile use for a DNA sample and one the Court was not willing to surrender for the sake of fidelity to the special needs doctrine.[217] The scientific and statutory safeguards in place

---

205 *King*, 569 U.S. at 461 ("By comparison to this substantial government interest and the unique effectiveness of DNA identification, the intrusion of a cheek swab to obtain a DNA sample is a minimal one. . . . The government interest must outweigh the degree to which the search invades an individual's legitimate expectations of privacy.").

206 *Id.* at 461–62.

207 Bertillon measurements were a set of ten measurements of an arrestee's body, along with notations of scars or other identifying marks, and an analysis of the arrestee's face. *Id.* at 457–58.

208 *See id.* at 449–61.

209 Ferguson v. City of Charleston, 532 U.S. 67, 99–100 (2001) (Scalia, J., dissenting).

210 *See id.* at 99.

211 *Id.* at 73 (majority opinion).

212 *King*, 569 U.S. at 474–76 (Scalia, J., dissenting).

213 *Id.* at 480–81.

214 *See id.* at 466, 480–81.

215 *See* discussion *supra* Part II.A.

216 Ferguson v. City of Charleston, 186 F.3d 469, 488 (4th Cir. 1999) (Blake, J., dissenting in part), *rev'd*, 532 U.S. 67 (2001).

217 *See King*, 569 U.S. at 480–81 (Scalia, J., dissenting).

were sufficient to convince the Court that no less desirable uses for DNA samples could result from their decision.[218]

The focus on use was possible in both cases because the searches at issue did not trouble the Court.[219] By breaking the searches down into two parts, one can see there is nothing inherently troubling about government officials possessing an individual's urine or cheek cells. The biological materials offer no significant information about a person unless they are tested or analyzed. However, in both cases, the searches were extremely limited. While urine tests can reveal a variety of medical facts about a person, the *Ferguson* tests revealed only whether the women had used cocaine.[220] King's DNA was searched only to reveal thirteen locus points that solely contained identifying information, not any other information that could have revealed his genetic predispositions.[221] Compare these searches with a more traditional search such as going through an arrestee's pockets or wiretapping a private conversation.[222] Both will reveal many more pieces of information than the urine tests and DNA processing in *Ferguson* and *King*. Since urine tests and DNA processing searches are limited to revealing a single piece of information about an individual, there is relatively little reason for the Court to worry about the searches themselves. All the potentially "unreasonable" actions relate to how the government can use the results of the subsequent analyses. Therefore, the Court based its decisions in *Ferguson* and *King* on how the government used the collected materials. In the Court's efforts to obscure the true bases for its decisions, it wrote two convoluted opinions.

C. *The Disclosure Cases*

Ferguson and *King* are the two cases that speak most directly to the Court's ability to impose use restrictions under the Fourth Amendment. Both cases center on law enforcement's use of collected information to initiate criminal proceedings. The below cases focus on a different use: public disclosure. The right to control one's personal information is a nebulous one. And the Court has not been clear where this right is even located in the Constitution, though the Fourth Amendment seems like a logical place.[223] These cases reflect the Court's instinct that even if a state actor is able to collect certain information from an individual, the Constitution places limits on how the state may use that information.[224]

---

218 *See id.* at 464–65 (majority opinion) (detailing the limited information contained in the "junk DNA" and the protections of the Act).

219 *See id*. at 469 (Scalia, J., dissenting); *Ferguson*, 532 U.S. at 76–77.

220 *Ferguson*, 186 F.3d at 474.

221 *King*, 569 U.S. at 464.

222 *See id*. at 446; *Ferguson*, 532 U.S. at 76.

223 *See* NASA v. Nelson, 562 U.S. 134, 146–47 (2011) (assuming that informational privacy implicates a constitutional right to privacy, without specifying any constitutional provisions).

224 *See, e.g.*, *id.* at 159.

1. *Whalen v. Roe*

In 1970, New York formed a commission to evaluate its drug-control laws.[225] The commission found that the existing system had certain problems.[226] It allowed patients to obtain addictive drugs from more than one doctor and for unscrupulous pharmacists to repeatedly refill a single prescription.[227] To remedy these problems, the state passed the New York State Controlled Substances Act of 1972.[228] The Act organized drugs by their potential for abuse.[229] Schedule I included drugs like heroin, while Schedule II included the most dangerous drugs doctors could prescribe, such as opium and opium derivatives.[230] The Act required that copies of all prescriptions for Schedule II drugs be sent to the New York State Department of Health in Albany.[231] These prescriptions were logged on an early computer system using magnetic tapes.[232] The magnetic tapes were kept in a locked cabinet and only accessed when the computer was offline (unconnected to any other computer).[233] Public disclosure of the patients' identities was strictly prohibited by the Act.[234]

Patients who regularly received Schedule II prescriptions challenged the Act.[235] The Supreme Court characterized the patients' concerns as twofold.[236] First, the patients felt having their information in the state's system would stigmatize them (one brief said having their illnesses "generally known" in this way "caused them acute discomfort and embarrassment").[237] Second, the patients feared the state disclosing their information.[238] The Court initially determined that the state had a "vital interest in controlling the distribution of dangerous drugs" that supported its decision to pass the Act.[239] The Court then held that the Act did not violate the Constitution because there was no evidence of a threat of improper disclosures, given the security measures and the Act's protections against disclosures.[240] The Court briefly determined that simply sharing the information at issue with the state was not constitutionally problematic because doing so was not "meaningfully distinguishable from a

---

225 Whalen v. Roe, 429 U.S. 589, 591 (1977).
226 *Id.* at 591–92.
227 *Id.* at 591.
228 *Id.* at 592.
229 *Id.*
230 *Whalen*, 429 U.S. at 592–93.
231 *Id.* at 593.
232 *Id.*
233 *Id.* at 594.
234 *Id.*
235 *Id.* at 595.
236 *Whalen*, 429 U.S. at 595 n.16.
237 *Id.* at 595 n.16; Appellees' Brief at 21, Whalen v. Roe, 429 U.S. 589 (1977) (No. 75-839).
238 *Whalen*, 429 U.S. at 595 n.16.
239 *Id.* at 598.
240 *Id.* at 601–02.

host of other unpleasant invasions of privacy that are associated with many facets of health care," and existing disclosure requirements were not significantly different from those in the Act.[241]

It was not clear which constitutional amendment was at issue in *Whalen*. The Court described privacy as involving "at least two different kinds of interests."[242] One was the freedom to make certain important decisions independently.[243] The first citation for this interest was to *Roe v. Wade*,[244] which was based on the Fourteenth Amendment.[245] The other interest was described as "the individual interest in avoiding disclosure of personal matters."[246] The first citation for this interest was Justice Brandeis's famous dissent in the Fourth Amendment case *Olmstead v. United States*,[247] where he discussed "the right to be let alone."[248] The second citation was to *Griswold v. Connecticut*[249] with a parenthetical quote: the "First Amendment has a penumbra where privacy is protected from governmental intrusion."[250] The Court included three additional citations to cases that involved the First, Fourth, Fifth, and Fourteenth Amendments.[251] Ultimately, the Court held that New York's Act did not violate "any right or liberty protected by the Fourteenth Amendment" and simultaneously addressed appellees' Fourth Amendment arguments in a footnote.[252]

This scattershot approach made some sense in the context of the 1970s. *Whalen* was decided four years after *Roe v. Wade*.[253] *Roe* significantly impacted the definition of privacy.[254] *Roe* approached the concept of a "right of privacy" extremely broadly:

> The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as *Union Pacific R. Co. v. Botsford*, the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual justices have, indeed, found at least the roots of that right in the First Amendment; in the Fourth and Fifth Amendments; in

---

241 *Id.* at 602.

242 *Id.* at 599.

243 *Id.* at 599–600.

244 410 U.S. 113 (1973).

245 *Whalen*, 429 U.S. at 600 n.26 (citing, inter alia, *Roe*, 410 U.S. at 164).

246 *Id.* at 599.

247 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

248 *Whalen*, 429 U.S. at 599 n.25 (citing *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting)).

249 381 U.S. 479 (1965).

250 *Whalen*, 429 U.S. at 599 n.25 (quoting *Griswold*, 381 U.S. at 483).

251 *Id.*

252 *Id.* at 603–04 n.32.

253 *See* Roe v. Wade, 410 U.S. 113, 113 (1973).

254 *See* Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 788 (1989) ("*Roe v. Wade* is probably the most important privacy case decided." (footnote omitted)).

> the penumbras of the Bill of Rights; in the Ninth Amendment; or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment.[255]

In this context, it is unsurprising that the *Whalen* Court was not overly concerned with pinning down the exact location of "the individual interest in avoiding disclosure of personal matters."[256] However, *Whalen* was the first decision to clearly annunciate such a right.[257] The decision itself is oddly noncommittal about the right, stating that "avoid[ing] unwarranted disclosures" is a "duty [that] arguably has its roots in the Constitution . . . in some circumstances."[258] The patients did not force the Court's focus on disclosure.[259] They simply objected to the state collecting their information and entering it into a computer.[260] The Court focused on disclosure and, in the process, create an uncertain new right of privacy.[261] This right looked beyond the traditional focus on government collection of material and dictated what the government could or could not do with information it had collected.[262]

2. *Nixon v. Administrator of General Services*

This new right appeared again just four months later in *Nixon v. Administrator of General Services*.[263] After President Nixon resigned, Congress passed the Presidential Recordings and Materials Preservation Act.[264] The Act required President Nixon to turn over all his presidential papers and recordings for archivists (from the executive branch) to sort through.[265] Some materials would be retained for the public, while any personal or private materials would be returned to President Nixon.[266] President Nixon challenged the Act on multiple constitutional grounds.[267]

The Court produced a lengthy opinion. One section was titled "Privacy."[268] The section purported to address President Nixon's Fourth and Fifth Amendment rights.[269] The Court discussed the President's rights solely in

---

255 *Roe*, 410 U.S. at 152 (citations omitted).

256 *Whalen*, 429 U.S. at 599.

257 *See* NASA v. Nelson, 562 U.S. 134, 138 (2011).

258 *Whalen*, 429 U.S. at 605.

259 *See* Roe v. Ingraham, 403 F. Supp. 931, 932 (S.D.N.Y. 1975), *rev'd sub nom.* Whalen v. Roe, 429 U.S. 589 (1977).

260 *Id.*

261 *See Whalen*, 429 U.S. at 605.

262 *Id.*

263 433 U.S. 425 (1977).

264 *Id.* at 429.

265 *Id.*

266 *Id.*

267 *Id.* at 430.

268 *Id.* at 455.

269 *See Nixon*, 433 U.S. at 455.

terms of the right announced in *Whalen*.[270] However, the Court was just as ambivalent about the right as it had been previously. Instead of announcing that a right to avoid disclosure of personal matters existed in a particular amendment, the Court stated: "One element of privacy has been characterized as 'the individual interest in avoiding disclosure of personal matters . . . .'"[271] The Court then analyzed the Act's protections against disclosures.[272] The government would not retain any purely private papers; the Act required regulations be promulgated that would minimize the intrusion into the President's private materials; the screening would be performed by discrete archivists; and the amount of private material was relatively small in any case.[273] Additionally, the Court based its holding on the fact that President Nixon was a public figure with no expectation of privacy in the majority of the materials; there was a strong public interest in preserving the materials; and there was simply no way to screen out the private materials without a team of professionals to sort the millions of pages and hours of recordings.[274] All these factors together persuaded the Court that President Nixon's "privacy claim" was without merit.[275]

Nixon is similar to *Whalen* in that both cases feature parties objecting to the government collecting information from them, and the Court choosing to instead focus on the possibility of disclosure.[276] The Court appeared to have an instinct in both cases that (1) collection of the information was unobjectionable and necessary from a pragmatic standpoint, and (2) there was nonetheless a legitimate privacy interest at stake.[277] In *Whalen*, the Court was not going to tell New York State that it could not collect important health-related information in a more efficient, centralized manner than existing reporting requirements allowed for. In *Nixon*, the Court was not going to strike down an Act regarding President Nixon's materials while Watergate and his resignation were still fresh in the country's memory. But the Court was also not willing to say that the parties lost all privacy interests in their materials once the government had collected them. It likely seemed too harsh, given the commonsense notion that privacy "is not a discrete commodity, possessed absolutely or not at all."[278] However, the Court had not previously placed restrictions, disclosure-related or otherwise, on what the government could do with material it had lawfully collected.[279] While the 1970s were a time when privacy rights had expanded in unexpected ways,[280] the Court had no

---

270 *Id.* at 457–59.

271 *Id.* at 457 (quoting Whalen v. Roe, 429 U.S. 589, 599 (1977)).

272 *Id.* at 459–65.

273 *Id.* at 459–64.

274 *Id.* at 465.

275 *Nixon*, 433 U.S. at 465.

276 *See id.* at 460; *Whalen*, 429 U.S. at 605.

277 *See Nixon*, 433 U.S. at 460; *Whalen*, 429 U.S. at 605.

278 Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

279 *See id.* at 751.

280 *See* Roe v. Wade, 410 U.S. 113, 154 (1973); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972).

reason to go further than society pushed them. So, for the next thirty-three years, not much was said about "the individual interest in avoiding disclosure of personal matters."[281]

3. *National Aeronautics & Space Administration v. Nelson*

The Court returned to the right introduced in *Whalen* in 2011. The issue arose with a background check form sent to government contractors working for NASA.[282] The form asked about employees' drug use and whether they had received any treatment for their drug use.[283] If the employees did not complete the forms, they would face termination.[284] Their responses were protected by the Privacy Act.[285] The Privacy Act prohibits any disclosures about a person without that person's written consent (subject to certain exceptions).[286]

The Supreme Court focused on the employees' informational privacy claim. The Court stepped carefully, "assum[ing], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*."[287] Justice Alito, writing for the Court, did not announce a standard for determining when an individual's informational privacy rights had been violated.[288] However, he stated that "whatever the scope of this interest, it does not prevent the Government from asking reasonable questions . . . in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure."[289]

The Court then went through a number of factors that spoke to the "reasonableness" of the questions, including the government's position as the plaintiffs' employer, and the questions' ability to further the government's interest as an employer.[290] Once the Court determined the questions were reasonable, it found that the challenged questions were "also subject to substantial protections against disclosure to the public."[291] The Court based its

---

281 *Whalen*, 429 U.S. at 599.

282 NASA v. Nelson, 562 U.S. 134, 139–40.

283 *Id.* at 141.

284 *Id.* at 140.

285 *Id.* at 142.

286 *Id.*

287 *NASA*, 562 U.S. at 138.

288 *Id.* at 159 ("In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the form consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy."); *id.* at 165 (Scalia, J., concurring) ("The Court decides that the Government did not violate the right to informational privacy without deciding whether there *is* a right to informational privacy, and without even describing what hypothetical standard should be used to assess whether the hypothetical right has been violated.").

289 *Id.* at 147–48 (majority opinion).

290 *Id.* at 148–55.

291 *Id.* at 155.

ultimate holding in favor of the government on *both* the reasonableness of the questions and the Privacy Act's nondisclosure requirement: "In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy."[292]

Justice Scalia and Justice Thomas concurred only in the judgment. Justice Scalia stated simply: "A federal constitutional right to 'informational privacy' does not exist."[293] He highlighted the fact that the employees failed to include a single citation to the Constitution in their brief to support their theoretical constitutional right.[294] He attacked *Whalen* and *Nixon* for failing to supply "any coherent reason why a constitutional right to informational privacy might exist."[295] Lastly, he attacked the Court for applying "a constitutional informational privacy standard without giving a clue as to the rule of law it [was] applying."[296]

Justice Scalia's arguments have real weight. The Court was unable to announce an existing informational privacy standard because *Whalen* and *Nixon* did not provide one.[297] The Court declined to announce a new standard but instead used factors that closely resembled the usual special needs factors. The special needs factors in *Vernonia* were (1) the individuals' reduced expectations of privacy; (2) the character of the intrusion; (3) the nature of the government's interest; and (4) the efficacy of the chosen means for meeting that interest.[298] In *NASA*, Justice Alito discussed (1) the government's position as the plaintiffs' employer (suggesting the employees had reduced expectations of privacy, just as the *Vernonia* students had in relation their school); (2) the similarity of the questions to those on private companies' background forms (i.e., the questions were not very intrusive); (3) the government's interest in performing background checks; and (4) the questions' ability to further the government's interest.[299]

Besides matching the special needs factors, the Court continually referred to "reasonableness" as the constitutional bar the questions needed to meet.[300] This is reminiscent of *Katz*'s "reasonable expectation of privacy" bar.[301] The "reasonableness" language and the special needs factors strongly

---

292 *Id.* at 159.

293 *NASA*, 562 U.S. at 160 (Scalia, J., concurring).

294 *Id.*

295 *Id.* at 164.

296 *Id.* at 166.

297 *Id.* at 165 ("The Court decides that the Government did not violate the right to informational privacy without deciding whether there *is* a right to informational privacy, and without even describing what hypothetical standard should be used to assess whether the hypothetical right has been violated.").

298 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–60 (1995).

299 NASA, 562 U.S. at 148–55.

300 *Id.* at 148, 151–52, 154–55, 159.

301 Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

suggest that the Court was imagining that the right to informational privacy lies in the Fourth Amendment.

The Court largely used a Fourth Amendment framework, and it also made a use restriction part of its holding: when asking sensitive questions like the ones at issue in the case, the government must have sufficient "safeguards against public disclosure."[302] The Privacy Act's safeguards were presented as essential to the Court's holding.[303] As in *Whalen* and *Nixon*, the Court suggested that without the statutory use restrictions, the Court would not have permitted the collection of the sensitive information.[304]

This opinion demonstrates that the Court is at least as concerned with individuals' sensitive information today as it was in 1977. At oral argument, there were four questions about what the government could ask (i.e., collect) about their employees.[305] For example, Justice Alito asked:

> [S]uppose the Government says, well, we want to know all about your diet; we want to know whether you smoke cigarettes; we want to know everything you read; we want to know what your hobbies are, what forms of entertainment you enjoy, sexual practices, every aspect of your private life, just because that gives us a better picture of who you are as an employee. Is that okay?[306]

There were also two questions about disclosure (i.e., how the government could use the collected information). The Court wanted to know exactly what prevented the government from finding out anything it wished about its employees, and what prevented the government from sharing that private information with the world.[307] The Court did not want either answer to be "nothing."[308]

The foregoing cases demonstrate the Court's willingness to impose use restrictions in certain cases.[309] The Court imposed a use restriction in *Ferguson* by prohibiting law enforcement from receiving and using pregnant women's drug test results to arrest them.[310] The four dissenting Justices in *King* would have forbidden arrestees' DNA from being used to solve old crimes.[311] And the Justices in the disclosure cases all recognized a restriction on when state actors may disclose individuals' personal information.[312] The

---

302 *NASA*, 562 U.S. at 147–48 ("We hold, however, that, whatever the scope of this interest, it does not prevent the Government from asking reasonable questions . . . in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure.").

303 *Id.* at 159.

304 *Id.* at 155, 159.

305 Transcript of Oral Argument at 3–4, 10, 13–14, 23–25, 56, NASA v. Nelson, 562 U.S. 134 (2011) (No. 09-530).

306 *Id.* at 13.

307 *Id.* at 10–11, 13, 57–58.

308 *See id.*

309 *See* discussion *supra* Part II.A.

310 Ferguson v. City of Charleston, 532 U.S. 67, 84–86 (2001).

311 *See* discussion *supra* Part II.B.

312 *See* discussion *supra* Part II.C.

next Part broadens the context of this trend toward use restrictions and explains why the pull towards use restrictions will become greater over time.

III. THE EVER-STRONGER PULL TOWARDS USE RESTRICTIONS

The Court has been willing to explore use restrictions previously and will find itself increasingly drawn to use restrictions in the future. New technologies will leave the Court little choice. The Court's Fourth Amendment doctrines are currently built around regulating collection: can an officer look through your trash,[313] aerially inspect your backyard,[314] or pat down your pockets?[315] Previously, when the Court regulated a new technology used by law enforcement, it was a technology that enabled more collection: beepers to track a suspect's location,[316] drug sniffing dogs,[317] or heat-vision goggles to spot the powerful lamps used to grow marijuana.[318] The existing collection-regulating doctrines could be applied to these new technologies because all they did was enable additional or easier collection. A beeper made it easier to track a suspect, but it was analogous to collecting the same information by having an unmarked police car follow the suspect around.[319] When faced with two beeper cases, the Court could utilize its existing collection-regulating doctrines to resolve the cases.[320] Existing doctrines said the police could freely collect information about individuals by observing them on the street, but the police could not freely collect information when an individual was at home.[321] The beeper cases were resolved accordingly: tracking beepers are permissible to use in public without a warrant, but they must be turned off if they enter a suspect's home.[322]

Today, new technologies are increasingly not technologies that enable new collection methods. They are technologies that enable novel uses of old collection methods. Cameras have existed for a long time; networks of cameras blanketing an entire metro area that are equipped with facial recognition technology have not.[323] Such a network could allow law enforcement to search for any individual, anywhere in a city, going back for weeks or

---

313 *E.g.*, California v. Greenwood, 486 U.S. 35, 39 (1988).

314 *E.g.*, California v. Ciraolo, 476 U.S. 207, 209 (1986).

315 *E.g.*, Terry v. Ohio, 392 U.S. 1, 12 (1968).

316 *E.g.*, United States v. Knotts, 460 U.S. 276, 277 (1983).

317 *E.g.*, United States v. Place, 462 U.S. 696, 697–98 (1983).

318 *E.g.*, Kyllo v. United States, 533 U.S. 27, 29 (2001).

319 *Knotts*, 460 U.S. at 285.

320 *See* United States v. Karo, 468 U.S. 705, 712 (1984); *Knotts*, 460 U.S. at 281–82.

321 *Knotts*, 460 U.S. at 282.

322 *Karo*, 468 U.S. at 716–17; *Knotts*, 460 U.S. at 285.

323 *See* Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017, 2:23 PM), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/.

months, depending on how much cheap data storage the city invested in.[324] An officer would not need to focus on an individual in real time, but only search the recorded footage for the individual after the fact. This new capability has serious privacy implications. New York City is already part of the way to having this type of blanket surveillance. A decade after 9/11, the city launched the "Domain Awareness System."[325] The system gives officers access to cameras across the city.[326] The city saves the video from its cameras for thirty days, and officers do not need a warrant to search through the stored video for any purpose.[327]

Algorithms that are a set of steps followed by a computer to solve a problem[328] also raise new privacy concerns. The Chicago Police Department utilizes complex algorithms to determine which people in Chicago are most likely to shoot someone, or be shot themselves.[329] It took the Department years to disclose all the various factors the algorithm uses to determine who should be on the "hot list," and it still does not describe or share the algorithm itself.[330] The Department uses the list to try to stage social work–like interventions, where they warn individuals of their high risk for being involved in violent crime and offer them opportunities to change the direction of their lives.[331] However, it is not difficult to imagine a more problematic use for such information, such as targeting suspects to be followed à la "Minority Report" pre-crime units.[332] Professor Andrew Guthrie Ferguson notes that by creating a kind of "big data suspicion," certain individuals will always be at risk for being stopped and will be forced to bear a "digital 'scarlet letter.'"[333]

---

324 *See id.*

325 Rocco Parascandola & Tina Moore, *NYPD Unveils New $40 Million Super Computer System that Uses Data from Network of Cameras, License Plate Readers and Crime Reports*, N.Y. DAILY NEWS (Aug. 8, 2012, 8:50 PM), http://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135.

326 *Id.*

327 Chris Francescani, *NYPD Expands Surveillance Net to Fight Crime As Well As Terrorism*, REUTERS (June 21, 2013, 11:24 AM), https://www.reuters.com/article/us-usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idUSBRE95K0T520130621.

328 *Algorithm*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/algorithm, (last visited Jan. 23, 2018).

329 *See* John Buntin, *Social Media Transforms the Way Chicago Fights Gang Violence*, GOV'T TECH. (Sept. 30, 2013), http://www.govtech.com/public-safety/Social-Media-Transforms-the-Way-Chicago-Fights-Gang-Violence.html; Davey, *supra* note 8.

330 *See* Jeff Asher & Rob Arthur, *Inside the Algorithm that Tries to Predict Gun Violence in Chicago*, N.Y. TIMES (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html?_r=1; Davey, *supra* note 8.

331 Asher & Arthur, *supra* note 330.

332 "The Minority Report" is a Philip K. Dick short story. It is set in a future where crime can be predicted, and a PreCrime Division of the police department arrests citizens who supposedly will commit crimes in the near future. PHILIP K. DICK, THE MINORITY REPORT (1956).

333 Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PENN. L. REV. 327, 401 (2015).

Other police departments have moved beyond looking at likely criminals and are utilizing algorithms to predict the behavior of any citizens they come into contact with. Some police departments use a program called "Beware" that color-codes citizens according to their "threat score."[334] Beware scours billions of records to decide if a person will present a green, yellow, or red level threat to officers.[335] Beware is more opaque than Chicago's hot list, as the factors that are used to calculate a person's threat score are not disclosed.[336]

Similarly, in one town in Minnesota, the police department has given officers an app for their phones so that when they approach any citizen, they can see if that citizen has any type of connection to someone with a criminal record.[337] At a traffic stop, an officer can immediately find out if the woman behind the wheel with no criminal record nevertheless has or had a boyfriend who did have a criminal record.[338] The police department has not revealed what records it gathers to power this app, or exactly how the police might treat individuals differently if they happen to be one or two steps removed from someone with a criminal record, or what other information officers might be able to instantly access about a person.[339]

These programs cannot be regulated by prohibiting an antecedent collection. The algorithms largely utilize the police departments' own records, along with public records, and some unknown number of private records.[340] The police obviously will have access to their own records and public records. If the Court wishes to restrict uses like Chicago's hot list or Beware, it will need to move beyond the approach in the special needs cases, where a use can speak to the reasonableness of the antecedent collection. The Court could look to the Fourteenth Amendment,[341] but due process restrictions alone are unlikely to answer all of the Court's concerns. Professor Tal Zarsky has observed that due process requires "a relatively high threshold of harm—

---

334 Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.

335 *Id.*

336 *See id.*

337 Maya Rao, *Rochester Hopes Predictive Policing Can Steer Juveniles Away from Crime*, STAR TRIB. (Oct. 24, 2014, 11:18 PM), http://www.startribune.com/rochester-police-plan-to-target-at-risk-teens-raises-concerns/280385202/.

338 *See id.* (explaining that police officers have access to information about car owners and "people one or two degrees of separation from that person")

339 *See id.*

340 *Id.*; Davey, *supra* note 8.

341 *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 1 (2014) (advocating for due process protections when automated scoring algorithms make predictions that significantly affect individuals' lives, such as credit scores); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1249, 1519–20 (2008) (advocating for due process protections in the administrative law context where algorithms drive decisions that impact individuals' rights, such as by placing them on the no-fly list).

to life, liberty, or property."[342] This threshold is usually not met by the type of algorithmic modeling done for Beware or Chicago's hot list.[343]

Other commenters have expressed serious concerns about the impact of new technologies on the Fourth Amendment. Professor Elizabeth Joh has called for a reexamination of the Court's long-standing assumptions about the lack of Fourth Amendment protections in public areas.[344] Given law enforcement's enhanced abilities, and Congress's inaction, Professor Joh argues that the public view doctrine should be altered, but she does not advocate for a specific approach.[345] Professor Jane Bambauer is more specific, arguing that bulk data collection should be considered an unreasonable Fourth Amendment search, unless a collection program has certain restraints.[346] Professor Bambauer does not make a distinction between collection and use, but she proposes regulating new technologies by restricting the access and use of third party records.[347]

The Court's wariness of law enforcement's enhanced abilities to go out and independently collect, store, and analyze data is most evident in the 2012 case, *United States v. Jones*.[348] The case concerned a GPS tracking device installed under the defendant Antoine Jones's car.[349] The police officers monitoring Jones had actually acquired a warrant to secretly install the device, but they failed to attach the device within the time and geographical limits set by the warrant.[350] They warrantlessly used the device to track Jones for twenty-eight days.[351] He was ultimately indicted and convicted of various drug charges.[352] Jones challenged the use of the evidence produced by the tracking device on Fourth Amendment grounds.[353]

Justice Scalia wrote the majority opinion for the Court.[354] He chose to ignore the thorny Fourth Amendment issues addressed by the lower courts.[355] Instead, he decided the case based on the trespass of placing the GPS device on Jones' car.[356] Because the officers "physically occupied private property

---

342 Tal Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1546 (2013).

343 *See id.*

344 Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 62–63 (2014).

345 *See id.*

346 Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 253–57 (2015).

347 *Id.*

348 565 U.S. 400 (2012).

349 *Id.* at 402.

350 *Id.* at 402–03.

351 *Id.* at 403.

352 *Id.*

353 *See id.* at 402–04.

354 *Jones*, 565 U.S. at 402.

355 *See id.* at 406.

356 *Id.* at 405–08. Commenters have described *Jones* as Justice Scalia's attempt to "resurrect" the trespass test in the Fourth Amendment context. *E.g.*, J. Bryan Boyd, *Arrested Development in Search Law: A Look at Disputed Consent Through the Lens of Trespass Law in a Post-Jones Fourth Amendment—Have We Arrived at Disputed Analysis?*, 46 SETON HALL L. REV. 1, 10 (2015); Andrew Guthrie

for the purpose of obtaining information," their actions constituted a warrantless search.[357] Justice Sotomayor concurred with the majority opinion, while Justices Alito, Ginsburg, Breyer, and Kagan concurred only in the result.[358]

In these two concurrences, five Justices moved beyond the narrow bounds of the majority opinion to form what other courts have called *Jones*'s "shadow majority."[359] They demonstrated that a majority of the Court is sufficiently concerned about law enforcement's use of modern surveillance technologies to consider relatively novel doctrinal solutions.

Justice Alito's concurrence expressed concern about the expansion of police surveillance due to new technologies and the cheaper cost of surveilling individuals long term.[360] He then went on to utilize *Katz*'s reasonable expectation of privacy framework in a novel fashion.[361] The *Katz* standard is usually applied to a person's possessions or a discrete action in a specific context, such as Katz's expectation of privacy in his phone booth calls or a passenger's expectation of privacy in his bus luggage.[362] Justice Alito's formulation of the *Katz* standard was far more expansive because it spoke to reasonable expectations about what society at large thinks law enforcement officers should do.[363] Justice Alito viewed the relevant expectation of privacy to be that "law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period."[364] A traditional application of *Katz* leads to a bag or a phone call in a specific setting being off-limits without a warrant.[365] Justice Alito's application of *Katz* could lead to entire police practices being off-limits, at least for most crimes.[366] Justice Alito's opinion was joined by three other Justices, and Justice Sotomayor clearly shared many of his concerns.[367] This makes five Justices who were willing to expand *Katz* to encompass reasonable

---

Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1308 (2014); Priscilla J. Smith, *Much Ado About Mosaics: How Original Principles Apply to Evolving Technology in* United States v. Jones, 14 N.C. J.L. & TECH. 557, 565–68 (2013).

357 *Jones*, 565 U.S. at 404–05.

358 *Id.* at 401.

359 United States v. Stimler, 864 F.3d 253, 276 (3d Cir. 2017) (Restrepo, J., concurring) (quoting In re Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted], 40 F. Supp. 3d 89, 92 (D.D.C. 2014)), *vacated in part sub nom.* United States v. Goldstein, 902 F.3d 411 (3d Cir. 2018).

360 *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment).

361 *Id.* at 430–31.

362 Bond v. United States, 529 U.S. 334, 338–39 (2000) (applying the *Katz* standard to a bus passenger's bag placed in an overhead bin).

363 *See Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment).

364 *Id.*

365 *See, e.g.*, *Bond*, 529 U.S. at 338–39; *Smith*, 442 U.S. at 741.

366 *See Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment) (stating that "longer term GPS monitoring in investigations of *most offenses* impinges on expectations of privacy" (emphasis added)).

367 *Id.* at 418; *id.* at 414–15 (Sotomayor, J., concurring).

expectations about how law enforcement officers may operate—in other words, how officers may collect or use information.[368]

In her concurrence, Justice Sotomayor considered the relevant expectation of privacy to be a person's expectation about his or her public movements viewed as a whole.[369] This is also more expansive than the traditional *Katz* inquiry about an item in a specific situation, if not as expansive as Justice Alito's formulation of the *Katz* standard. Six years later, in *Carpenter v. United States*,[370] the Court treated Justice Sotomayor's formulation of the reasonable expectation of privacy as virtually settled law: "A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements."[371] This was key to the reasoning in *Carpenter*—the Court concluded that the government was not entitled to acquire the defendant's cell-site location information from his cell phone service provider without a warrant because of this reasonable expectation of privacy.[372] In *Carpenter*, a majority of the Court was not willing to allow a relatively new technology to diminish Americans' privacy, and so the Court revised the relevant Fourth Amendment doctrine accordingly.[373]

The *Carpenter* Court's revised Fourth Amendment doctrine was the much-maligned third party doctrine, which applies when law enforcement acquires records from a third (nongovernmental) party.[374] However, revising the third party doctrine will only help protect privacy when data are collected or held by a third party; it will not help when government agents themselves collect data. If the Court now feels it must also expand privacy protections in cases of government surveillance, then it will need to take additional steps. The question is then how the Court would choose to frame and justify these future additional steps. The next Part makes the case that the best course for the Court to follow is the most straightforward one: to openly impose use restrictions.

---

368 *Id.*; *id.* at 418, 430 (Alito, J., concurring in judgment).

369 *Id.* at 416 (Sotomayor, J., concurring).

370 138 S. Ct. 2206 (2018).

371 *Id.* at 2216. While Justice Roberts attributed this formulation to both concurrences, it was Justice Sotomayor's concurrence that frames the expectation of privacy as "a reasonable societal expectation of privacy in the sum of one's public movements." *Jones,* 565 U.S. at 416 (Sotomayor, J., concurring).

372 *Carpenter*, 138 S. Ct. at 2219.

373 Justice Roberts, writing for the majority, seemed particularly motivated by the fact that the data at issue could be "detailed, encyclopedic, and effortlessly compiled." *Id.* at 2216. He noted that cell-site location data were "continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation" and therefore "this newfound tracking capacity runs against everyone." *Id.* at 2218. Justice Roberts has previously expressed concern that the Justices themselves could be continually tracked without a warrant. Transcript of Oral Argument at 9, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259).

374 *See, e.g.*, Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 96 HASTINGS L.J. 1039, 1044 (2018) (calling the third party doctrine "discredited"); Rebecca Lipman, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 481 (2014) ("[T]he judiciary should revisit the third party exception sooner rather than later.").

IV. WHY THE COURT SHOULD OPENLY IMPOSE USE RESTRICTIONS

Much ink has been spilled over the history of the Fourth Amendment.[375] Commenters largely agree that the Founders were greatly concerned with officers' discretion and the scope of searches and seizures.[376] Patrick Henry warned that without some new restriction, government agents could "go into your cellars and rooms, and search, ransack, and measure, every thing [sic] you eat, drink, and wear."[377] In England, the dangers of the government indiscriminately going through a person's papers had already been recognized: "Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection."[378]

The Fourth Amendment addressed these concerns. It states that the people have a right to be secure in "their persons, houses, papers, and effects."[379] "Effects" meant any personal possession, possibly extending to commercial goods.[380] This list covered virtually everything a person had in colonial times: himself, his house, his papers, and all of his possessions. People in his town might know a good deal about him, and a few local shopkeepers might know some of his purchasing habits. But a man's private thoughts, communications, and life history were recorded chiefly in his own mind and in his own papers.

Today, solely protecting "persons, houses, papers, and effects" does not sufficiently address the Framers' concerns. Law enforcement has far greater capabilities than the Founders ever imagined, as evidenced by the lack of clear Fourth Amendment protections in *Jones* and *King*.[381] Tinkering with the third party doctrine will not prevent systems like New York City's Domain Awareness System, with cameras covering the city,[382] or the creation of secret algorithms that are used to psychologically profile individuals.[383] As technology advances, the Fourth Amendment's once-comprehensive list of "persons, houses, papers, and effects"[384] will become more and more limited.

---

375 *See, e.g.*, WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING (2009); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181 (2016); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994).

376 *See* Donohue, *supra* note 375, at 1191; Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1058 (2011); Thomas Y. Davies, *The Fictional Character of Law-and-Order Originalism: A Case Study of the Distortions and Evasions of Framing-Era Arrest Doctrine in* Atwater v. Lago Vista, 37 WAKE FOREST L. REV. 239, 250 (2002).

377 THE DEBATES IN THE SEVERAL STATE CONVENTIONS, ON THE ADOPTION OF THE FEDERAL CONSTITUTION 448–49 (Jonathan Elliot ed., 2d ed., vol. III 1891).

378 Entick v. Carrington, 19 Howell's State Trials 1029, 1066 (C.P. 1765).

379 U.S. CONST. amend. IV.

380 Davies, *supra* note 376, at 707–09.

381 *See* discussion of King *supra* Part II.B and discussion of Jones *supra* Part III.

382 *See* Francescani, *supra* note 327.

383 *See* Asher & Arthur, *supra* note 330.

384 U.S. CONST. amend. IV.

Professor Christopher Slobogin sees these advances and the Court's lack of responsiveness to them as contributing to the Fourth Amendment's "increasing irrelevance."[385] The Amendment could become only a partial protection for what the Court has previously called "the privacies of life."[386] Partial protection is not what the Founders had in mind.

It is up to the Court to decide if it wishes the Fourth Amendment to maintain the strength it had when it was written. If the Court allows technology to diminish the Amendment, then the Fourth Amendment can simply become less relevant. In an age where some proclaim, "Privacy is dead, get over it,"[387] it is arguably appropriate for the Fourth Amendment to offer only limited protections against government intrusions.

But this is not the path the Court has chosen so far. New technologies have always had the potential to put pressure on the Fourth Amendment, depending on the technology at issue. *Katz* itself had to go beyond the list of "persons, houses, papers, and effects" to protect Charlie Katz's phone call.[388] Katz's conversation was not a person, house, paper, or effect.[389] It was information.[390] The Court therefore reached beyond the enumerated list and created the reasonable expectation of privacy standard.[391] The Court moved beyond the text of the Fourth Amendment to adhere to its spirit.[392]

The Court has openly expressed its desire to maintain the strength of the Fourth Amendment.[393] In *Kyllo v. United States*,[394] Justice Scalia (writing for the Court) recognized that new technologies could "shrink the realm of guaranteed privacy."[395] He consequently wrote a rule of decision based on the

---

385 CHRISTOPHER SLOBOGIN, IS THE FOURTH AMENDMENT RELEVANT IN A TECHNOLOGICAL AGE?, GOVERNANCE STUDIES AT BROOKINGS 2 (2010), https://www.brookings.edu/wp-content/uploads/2016/06/1208_4th_amendment_slobogin.pdf.

386 Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Boyd v. United States, 116 U.S. 616, 630 (1886).

387 Matt Hamblen, *McNealy Calls for Smart Cards to Help Security*, COMPUTERWORLD (Oct. 12, 2001, 1:00 AM), http://www.computerworld.com/article/2585627/security0/mcnealy-calls-for-smart-cards-to-help-security.html.

388 *See Katz*, 389 U.S. at 365 (Black, J., dissenting) (arguing that the majority holding is wrong because unlike "persons, houses, papers, and effects," a conversation is not tangible and thus cannot be searched or seized).

389 *Id.*

390 *Id.* at 365–66 (arguing that unlike "persons, houses, papers, and effects," a future conversation is information that cannot be "particularly describ[ed]," as required by the Fourth Amendment to obtain a warrant).

391 *Id.* at 360 (Harlan, J., concurring)

392 *See id.* at 351 (majority opinion) (explaining that "the Fourth Amendment protects people, not places").

393 *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

394 533 U.S. 27 (2001).

395 *Id.* at 34.

prevalence of any new technology.[396] He stated that his rule "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[397]

In *Riley v. California*,[398] Chief Justice Roberts wrote for the Court in a 9-0 decision.[399] *Riley* is a 2014 case.[400] In 2014, smartphones were a relatively new technology putting pressure on the Fourth Amendment.[401] Consequently, the Court held that unlike virtually any other item, a cell phone could not be searched incident to arrest.[402] Chief Justice Roberts placed the Court's decision in the context of the strength of the Fourth Amendment during the founding era:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.[403]

"Information" is not mentioned in the Fourth Amendment.[404] Yet Chief Justice Roberts said that "information" is the thing the Founders fought to protect.[405] The Chief Justice was not focused on the text of the Fourth Amendment; he was focused on the spirit and the goals of the Fourth Amendment.[406] He was not afraid to read this additional protection into the Amendment if it adhered to that spirit and advanced the Amendment's goals. He continued to follow this path in *Carpenter* in 2018. While voting with the four more liberal Justices, the Chief Justice quoted Justice Scalia and maintained an originalist stance:

> We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has

---

396 *Id.* at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

397 *Id.* at 34.

398 134 S. Ct. 2473 (2014).

399 *Id.* at 2479.

400 *Id.* at 2473.

401 In 2014, 59 percent of American adults had a smartphone. PEW RESEARCH CENTER, MOBILE FACT SHEET (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

402 *Riley*, 134 S. Ct. at 2495.

403 *Id.* at 2494–95 (citation omitted).

404 *See* U.S. CONST. amend. IV.

405 *See Riley*, 134 S. Ct. at 2495 (stating that the fact technology now allows an individual to carry private information in a cell phone does not make that information less worthy of Fourth Amendment protection).

406 *See id.*

> sought to "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[407]

As members of the Court across the ideological spectrum seek to uphold the spirit of the Fourth Amendment, they will feel the need to impose use restrictions going forward to prevent law enforcement from ascertaining, "more or less at will, [an individual's] political and religious beliefs, sexual habits, and so on."[408] Unfortunately, the Court's former approaches to creating use restrictions are seriously flawed. Each former approach is briefly described below. Following these descriptions, the Article proposes a new, two-track approach to openly imposing use restrictions.

D. *Three Former Approaches to Creating Use Restrictions*

1. Obfuscating the Holding

One way to impose use restrictions is by obfuscating the actual holding of a case. *Ferguson* is the one case where a majority of the Court found that a specific use was unconstitutional.[409] The Court prohibited a state hospital from sharing pregnant women's urine test results with law enforcement.[410] The Court did not openly impose a use restriction. Instead, the Court held that the entire policy was an unconstitutional search.[411] As Justice Scalia pointed out, though, the policy involved three discrete steps: collecting the women's urine, testing the urine, and sharing the test results with law enforcement.[412] Justice Scalia incredulously asked if the Court could "really believe (or even *hope*) that, once invalidation of the program challenged here has been decreed, drug testing will cease?"[413] The answer was clearly "no."[414] The Court's holding explicitly relied on the "extensive involvement of law enforcement officials at every stage of the policy."[415] Without law enforcement's involvement, the policy would not have been unconstitutional.[416]

---

407 Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (alteration in original) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

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

409 *See supra* Part II.A.

410 Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001).

411 *Id.* at 86.

412 *Id.* at 92 (Scalia, J., dissenting).

413 *Id.* at 100.

414 *See id.*

415 *Id.* at 84 (majority opinion).

416 *Ferguson*, 532 U.S. at 85 ("[Respondents'] motive . . . cannot justify a departure from Fourth Amendment protections, given the pervasive involvement of law enforcement with the development and application of the MUSC policy.")

Therefore, the sole effect of the Court's holding was to prohibit the sharing of the test results with law enforcement.[417]

The *Ferguson* Court imposed a use restriction by holding that the entire policy was an unconstitutional search.[418] The Court did so even though the only part of the policy the Court actually found objectionable was the sharing of results with law enforcement.[419] This obfuscating approach provided no clear guidance for state actors going forward. It did not advance the Court's existing Fourth Amendment case law. And it muddied the special needs doctrine by creating an implausible "immediate objective" versus "ultimate goal" framework to justify its holding.[420] If the Court chose to continue creating use restrictions by hiding what it was actually doing, the Court would make Fourth Amendment law significantly less coherent.[421] The Court should not impose use restrictions in a way that makes it impossible to understand what Fourth Amendment rules are being created.

2. Announcing a Use Restriction Without a Constitutional Explanation

A second way to impose use restrictions is to explicitly announce a restriction without providing a constitutional basis for it. The disclosure cases, *Whalen*, *Nixon*, and *NASA*, are discussed above in Part II.C. They all pursue the peculiar course of announcing an "individual interest in avoiding disclosure of personal matters"[422] without explaining where in the Constitution this interest comes from. The Fourth, Fifth, and Fourteenth Amendments were all possibilities in *Whalen*.[423] *Nixon* seemed to narrow it down to the First, Fourth, or Fifth Amendment.[424] *NASA*, the most recent case, appeared to lean toward the Fourth Amendment.[425] However, the *NASA* Court would not commit to whether an informational privacy right actually existed.[426] The Court

---

417 *See id.* at 85–86.

418 *Id.* at 85.

419 *Id.* at 84.

420 *Id.* at 82–84.

421 *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011) (noting scholars already complain that the Fourth Amendment is "'a mess,' 'an embarrassment,' and 'a mass of contradictions'" (footnotes omitted) (first quoting Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149 (1998); then quoting AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 1 (1997); then quoting Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 (1985))).

422 Whalen v. Roe, 429 U.S. 589, 599 (1977).

423 *See id.* at 599 n.25.

424 Nixon v. Admin. of Gen. Servs., 433 U.S. 425, 455 (1977).

425 *See* NASA v. Nelson, 562 U.S. 134, 158–59 (2011) (speaking in terms of reasonableness and a right to informational privacy).

426 *Id.* at 147 n.10.

"assum[ed], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*."[427]

The privacy right at issue is a use restriction. The right restricts state actors from freely disclosing sensitive information about individuals.[428] The advantage of this approach is that it clearly announces a use restriction: the government can collect information, but it cannot engage in "unwarranted disclosures" of sensitive information.[429] There is no hiding the ball like there was in *Ferguson*. However, the disadvantages of this approach are overwhelming. By declining to specify where this right comes from, or even to confirm that it definitely exists, the Court creates a massive amount of uncertainty. The Court cannot impose future use restrictions by repeatedly creating new, free-floating rights, which may or may not actually exist. Such an approach would simply be incompatible with building a functional body of case law.

3. The Mosaic Theory

The third approach to use restrictions that the Court has contemplated is the mosaic theory. The theory is not mentioned by name in *Jones*, but both concurrences consider it.[430] The mosaic theory posits that a lawful collection technique, such as surveilling a man in public, can become unlawful if it "reveal[s] an intimate picture of his life."[431] Justice Sotomayor imagined an unconstitutional mosaic could be formed if state actors acquired sufficient information about an individual such that they could "ascertain, more or less at will, [an individual's] political and religious beliefs, sexual habits, and so on."[432] Justice Alito seemed to favor a chronological-based approach to the theory, wherein a collection technique would become unconstitutional if used for a certain amount of time.[433] Justice Alito stated, "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[434]

---

427 *Id.* at 138.

428 *See id.* (explaining the *Whalen* description of an "interest in avoiding disclosure of personal matters" and resting its holding in part on the fact that the government's statutorily limited ability to release sensitive information about its employees (quoting Whalen v. Roe, 429 U.S. 589, 599–600 (1977))).

429 *Id.* at 156–57.

430 United States v. Jones, 565 U.S. 400, 414–15 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in judgment).

431 United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

432 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

433 *See id.* at 418–19 (Alito, J., concurring in judgment).

434 *Id.* at 430. Justice Alito did not favor the time-based approach in *Carpenter*, which set a seven-day limit, as he believed the core issue of the case was addressed by the Stored Communications Act, not the Fourth Amendment. Carpenter v. United States, 138 S. Ct. 2206, 2266–67 (2018) (Alito, J., dissenting).

The mosaic theory has since been actively discussed by academics.[435] Many commenters have concluded that the theory is unworkable.[436] Professor Orin Kerr has highlighted four major questions about the theory:

> (1) The Standard Question. . . . What test determines when a mosaic has been created? The three pro-mosaic opinions in *Maynard/Jones* suggested three different standards . . . . Is data collection enough, or is subsequent analysis and use also required? If the latter, what are the constitutional standards for data analysis and disclosure?
>
> (2) The Grouping Question. . . . The mosaic theory groups conduct that is not a search and asks if the nonsearches considered together cross the line to become a search. . . . Which surveillance methods prompt a mosaic approach? Should courts group across surveillance methods? If so, how? What is the half-life of a mosaic search?
>
> (3) Constitutional Reasonableness. . . . Mosaic searches do not fit an obvious doctrinal box for determining reasonableness. The nature of the mosaic is that each mosaic will be different, potentially requiring different kinds of reasonableness analyses for each one. . . .
>
> (4) Remedies for Mosaic Violations. . . . Does the exclusionary rule apply? If so, does the rule extend over all of the mosaic or only the surveillance that crossed the line to trigger a search? Who has standing to challenge mosaic searches? . . .[437]

This Article does not attempt to improve upon the excellent analysis by Professor Kerr and others. The mosaic approach is a tempting option for creating use restrictions because it speaks to the heart of the problem: aggregation.[438] The "tiles" in the mosaic were always available to law enforcement: people are visible wherever they go in public, there are no restrictions on speaking to a person's friends or coworkers to learn about their habits or beliefs, and a lot of sensitive information is available in public and semipublic files online.[439] These tiles, and law enforcement's freedom to collect them, are still not a problem. The *Maynard* and *Jones* opinions correctly home in on the new problem: the ease of taking these disparate tiles and then aggregating them into a mosaic that reveals a person's entire life.[440]

---

435 *See, e.g.*, Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 311 (2012); Paul Ohm, *The Life of Riley (v. California)*, 48 TEX. TECH. L. REV. 133, 135–36 (2015); Courtney E. Walsh, *Surveillance Technology and the Loss of Something A Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 232 (2012) (noting "commentators have articulated several criticisms of the 'mosaic theory' that can be grouped under the general heading of 'unworkability'"); Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1735 (2011). *But see* Jace C. Gatewood, *District of Columbia Jones and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504, 535–36 (2014) (endorsing the mosaic theory in spite of its problems); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 424 (2013) (endorsing the mosaic theory in spite of its problems).

436 *See* sources cited *supra* note 435.

437 Kerr, *supra* note 435, at 329–30.

438 *Id.* at 320.

439 *Cf. Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring).

440 Kerr, *supra* note 435, at 320.

It is understandable that the Court would want to address the problem head on by simply prohibiting the creation of mosaics. But for all the reasons Professor Kerr raises, it is hard to imagine how the Court would implement such an approach.[441] Gathering information to better understand suspects is a core aspect of any police investigation.[442] Police officers must be adept at understanding Fourth Amendment law to the extent that they must learn what parts of a car they can search during a traffic stop[443] and when they can pat someone down.[444] But they cannot be expected to recognize the moment that they have gathered enough information to ascertain an individual's political and religious beliefs at will—it is simply too amorphous a standard. Professor Slobogin has attempted to distill the mosaic theory into a workable legislative scheme that provides clear guidelines to officers: a targeted public search over twenty minutes long should require reasonable suspicion, and a targeted public search over forty-eight hours long should require probable cause (and a warrant, absent an exception).[445] However, a time-limited approach does not significantly limit a police officer's ability to quickly create a mosaic of facts that are not time dependent. For example, a person's political and theological leanings, social connections, and sexual preferences could be determined with some degree of accuracy simply by running the relevant online browsing records through a predictive algorithm.[446]

As Justice Alito noted in his *Jones* concurrence, the strongest privacy protections Americans have enjoyed thus far have not been statutory or constitutional.[447] They have been practical.[448] Practically speaking, the police would not previously have had the resources to track a suspected drug dealer twenty-four hours a day for a month.[449] Thanks to GPS technology, now that is possible.[450] The Court cannot roll back technological advances by regulating them based on their aggregate effect. A more direct approach is necessary.

---

441 *See id.* at 329.

442 *See* Lee Lofland, *An Insider's Look at the Police: What a Detective Does*, WRITER'S DIGEST (May 21, 2008), http://www.writersdigest.com/qp7-migration-books/police-procedure-excerpt.

443 *See* Arizona v. Gant, 556 U.S. 332, 356–57 (2009) (Alito, J., dissenting).

444 *See* Terry v. Ohio, 392 U.S. 1, 31–32 (1968) (Harlan, J., concurring).

445 Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 24 (2012).

446 Since private companies already create mosaic-like profiles for their own purposes, it could take less than twenty minutes for a police officer to gather the relevant data. *See, e.g.*, Jeremy B. Merrill, *Liberal, Moderate or Conservative? See How Facebook Labels You*, N.Y. TIMES (Aug. 23, 2016), http://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html?_r=0.

447 United States v. Jones, 565 U.S. 400, 429 (Alito, J., concurring in judgment).

448 *Id.*

449 *Id.*

450 *Id.* at 430.

E. *A Better Approach to Creating Use Restrictions*

This Part describes this Article's approach to imposing use restrictions. It then considers when this approach should be utilized, the impact of imposing use restrictions on individuals and institutions, and how use restrictions may be enforced.

1. Applying a Two-Track Approach to Use Restrictions.

The Court should openly impose use restrictions by utilizing a two-track approach. In cases where there has been a Fourth Amendment search, the Court has had the ability to prohibit the antecedent collection if the search was unreasonable.[451] A search is usually unreasonable if it was executed without a search warrant, but many exceptions may apply.[452] For example, testing students' urine was a search in *Vernonia,* but a warrant was not required because the special needs balancing led the Court to conclude the warrantless search was reasonable.[453] When the Court faces a case where an exception to the warrant requirement may apply, but the Court is concerned about how collected material is used, the Court should explicitly make the use of the material the determinative factor in the reasonableness analysis. This is essentially Professor Harold Krent's proposal,[454] and it is the "first track" under this Article's approach.[455]

The cases described *supra* Part II, *Ferguson* and *King*, would both fall into this first track, because in both cases the Court could prohibit the antecedent collection and testing of biological material.[456] Both cases would look quite different under this two-track approach, even if the end results for the parties were the same. As written, *Ferguson* avoided saying precisely what action it was prohibiting or what was the Fourth Amendment search at issue.[457] Opaque opinions make for poor precedent.[458] If *Ferguson* had been decided under the two-track approach, the Court could have explicitly held that the urine collection and testing was an impermissible search *because* the subsequent sharing with law enforcement rendered the antecedent search

---

451 *Id.* at 418–19.

452 Kerr, *supra* note 435, at 337.

453 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 660–65 (1995).

454 *See* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 64 (1995) (proposing that reasonableness can never be judged without considering how the government is using the seized items).

455 *See supra* Intro.

456 *See* Maryland v. King, 569 U.S. 435, 446 (2013); Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001).

457 The Court instead held that the hospital's entire prenatal drug testing "policy" was unconstitutional. *Ferguson*, 532 U.S. at 86 ("The Fourth Amendment's general prohibition against nonconsensual, warrantless, and suspicionless searches necessarily applies to such a policy.").

458 Orin S. Kerr, *A Theory of Law*, 16 GREEN BAG 2D 111, 111 (2012).

unreasonable. This would have precisely targeted the action the Justices believed violated the Fourth Amendment,[459] provided a clear rule, and clearly left the prenatal drug-testing program intact as long as law enforcement was not involved.[460]

In *King*, the majority opinion was written in such a way that ignored the central question of whether using an arrestee's DNA to solve an old rape case violated the arrestee's Fourth Amendment rights, much to the four dissenters' frustration.[461] If *King* had been decided utilizing the two-track approach, the Court could have tackled the relatively novel DNA use at the heart of the case head on and decided whether that specific use rendered the antecedent collection and genetic analysis unreasonable. This would have advanced the debate on what the government may do with individuals' genetic material without a warrant, rather than ignoring the issue by pretending that DNA samples are analogous to nineteenth-century corporal measurement techniques.[462]

Future cases involving situations like Chicago's hot list or New York City's Domain Awareness System will require a different track. In these cases, the collection of relevant records will not be a Fourth Amendment search. The Court cannot prohibit the police from accessing their own records, such as arrest records or fingerprints, without a warrant.[463] Nor can it prohibit the police from warrantlessly monitoring people on public streets.[464] Such restrictions would make basic policing tasks impossible. Therefore, the Court will not be able to impose a use restriction by analyzing the reasonableness of the antecedent collection as it would under the first track. Instead, the Court should find that certain uses are Fourth Amendment searches in their own right that can be analyzed for reasonableness independently of their antecedent collection. This is the "second track" of the two-track approach.[465]

---

459 The Court was clear that it was law enforcement's involvement that made the policy unconstitutional. *Ferguson*, 532 U.S. at 84 ("Given the primary purpose of the Charleston program, which was to use the threat of arrest and prosecution in order to force women into treatment, and given the extensive involvement of law enforcement officials at every stage of the policy, this case simply does not fit within the closely guarded category of 'special needs.'").

460 Justice Scalia incredulously asked in dissent if the majority could "really believe (or even *hope*) that, once invalidation of the program challenged here has been decreed, drug testing will cease?" *Id.* at 100 (Scalia, J., dissenting). The majority did not state that it wanted to stop screening at-risk pregnant women for drug use in the absence of law enforcement involvement. *Id.* at 85 (majority opinion).

461 *See King*, 569 U.S. at 470 (Scalia, J., dissenting).

462 *See id.* at 457 (majority opinion) (discussing the use of Bertillon measurements, a set of ten measurements of an arrestee's body, along with a notation of scars or other identifying marks, and an analysis of the arrestee's face).

463 ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-6.1(a), cmt. (3d. ed. 2013) [hereinafter ABA STANDARDS FOR CRIMINAL JUSTICE].

464 *See* Terry v. Ohio, 392 U.S. 1, 30 (1968).

465 *See supra* Intro.

The Court has already tentatively taken this track with urine tests, which it has suggested are "searches" in their own right.[466] Many uses readily fit the dictionary definition of "search" as an attempt to "look into . . . thoroughly in an effort to find or discover something."[467] For example, scouring all of an individual's social media posts or querying a surveillance database every time an individual appeared on a street camera can colloquially be described as "searches" violating an individual's reasonable expectations of privacy.[468] Once a use is categorized as a Fourth Amendment search, the Court can analyze that use independently and decide if it was a reasonable search, despite the lack of a warrant.

Calling a database query a Fourth Amendment search is novel, but it makes sense linguistically and constitutionally. Multiple commenters including Professors Akhil Amar and Slobogin have previously advocated for a "lay meaning" of the word "search."[469] Justice Alito's concurrence in *Jones* suggested that individuals can have reasonable expectations about how the police may investigate them.[470] Three other Justices joined his concurrence.[471] Under the *Katz* test, if an individual's reasonable expectation of privacy has been violated, a Fourth Amendment search has occurred.[472] Therefore, if a police officer queries a database in a way that violates an individual's reasonable expectation of privacy, then that query would be a Fourth Amendment search. This approach would allow the Court to target many problematic uses of modern-day surveillance without forbidding bulk collection[473] and without dipping into the morass of the mosaic theory.

Riley came very close to following the second track of the two-track approach.[474] The Court held that while it was "sensible" for Riley to concede

---

466 *See* Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001) (holding "the urine tests conducted by those staff members were indisputably searches within the meaning of the Fourth Amendment"); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995) (noting "state-compelled collection and testing of urine, such as that required by the Policy, constitutes a 'search' subject to the demands of the Fourth Amendment").

467 *Search*, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/search (last visited Feb. 3, 2018). Other commenters have advocated for the Court moving away from its own specialized definition of "search" to a more colloquial definition. *See, e.g.*, Slobogin, *supra* note 445, at 13–14.

468 *See* Slobogin, *supra* note 445, at 10.

469 Amar, *supra* note 375, at 768–70, 783; Slobogin, *supra* note 445, at 13–14; Akhil Reed Amar & Vikram David Amar, *I Always Feel Like Somebody's Watching Me: A Fourth Amendment Analysis Of The FBI's New Surveillance Policy*, FINDLAW (June 14, 2002) http://writ.news.findlaw.com/amar/20020614.html.

470 *See* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in judgment).

471 *Id.* at 418.

472 Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

473 If courts could target specific uses of collected data, they could exercise greater control over what police may do with incidentally collected data swept up by bulk collections. Professor Brian Owsley, who was formerly a magistrate judge, has advocated for greater notice and protection for innocent individuals' data that is swept up by bulk collections. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 J. CONST. L. 1, 46–47 (2013).

474 *See* Riley v. California, 134 S. Ct. 2473 (2014).

that the officers were permitted to seize his cell phone, the subsequent inspection of the data on the phone was an impermissible Fourth Amendment search.[475] To frame it in terms of the two-track approach, the Court believed it was not sensible to prohibit the antecedent collection (seizing the cell phone), so it moved to analyze the officer's subsequent inspection of the phone as an independent Fourth Amendment search.[476] The Court even highlighted that the cell phone could be used in other ways—the officers were free to physically inspect it for hidden dangers or place it in a Faraday bag to prevent remote deletion of data,[477] but they were not permitted to look at the data on the phone without a warrant.[478] This action was a separate search, subject to its own Fourth Amendment reasonableness analysis.[479]

The fact that examining the content of a cell phone so clearly resembles a "search" rather than a "use" makes *Riley* an imperfect example for the two-track approach. But *Riley* demonstrates the advantages of tackling the issue at the heart of a case head-on, which the two-track approach encourages.[480] While the majority opinions in *Ferguson* and *King* garnered only five votes, *Riley* was unanimous.[481] *Ferguson* and *King* are opaque cases with convoluted reasoning, while *Riley* roots its reasoning in Fourth Amendment precedent and the original scope of the Amendment's protection.[482] By being upfront about what troubles the Court (the vast amount of data on cell phones revealing an excess of information to arresting officers), the Court can clearly communicate its reasoning and create a bright-line rule in the process.[483] The next time the Court is faced with a case where an officer's actions raise Fourth Amendment issues and could potentially be characterized as a search, the Court would benefit from looking to *Riley* as an example.

The two-track approach presented here is superior to other methods of imposing use restrictions because it enables the Court to zero in on the action it finds constitutionally questionable, analyze its reasonableness, and create a clear rule regarding the specific action. It works in the same "sequential"

---

475 *Id.* at 2495.

476 *Id.* at 2493.

477 *Id.* at 2485, 2487.

478 *Id.* at 2495.

479 *See id.* at 2493.

480 *See Riley*, 134 S. Ct. at 2493.

481 *Id.* at 2479; Maryland v. King, 569 U.S. 435, 438 (2013); Ferguson v. City of Charleston, 532 U.S. 67, 69 (2001).

482 *See Riley*, 134 S. Ct. at 2483–84, 2494–95 (discussing search incident to arrest cases and cell phones in the context of the origins of the Fourth Amendment); *King*, 569 U.S. at 465; *Ferguson*, 532 U.S. at 85.

483 *See Riley*, 134 S. Ct. at 2494–95. Clear concerns will not always lead to clear rules, if the Court simultaneously tries addressing its concerns and preserving a troubled doctrine. *See* Carpenter v. United States, 138 S. Ct. 2206, 2232–33 (Kennedy, J., dissenting) (explaining that it is impossible to meaningfully distinguish cell-site location records, which the Court protected in *Carpenter*, from financial records, which the Court left unprotected under the third party doctrine).

manner as other Fourth Amendment doctrines, unlike the mosaic theory.[484] However, it would be disingenuous to suggest that the two-track approach is entirely different from the mosaic theory. Both are motivated by a concern about the power of aggregation.

Police officers have always aggregated information and then linked it in creative ways to discover a key element of a case. For example, once an officer puts together the information that a suspect has maxed out his credit cards, that he frequently receives brief late night phone calls from the same phone number, and that phone number belongs to a bookie, then the officer has discovered that the suspect likely has a serious gambling problem. The problem with the mosaic theory is that it tries to prevent this moment of discovery. An "intimate picture of [the suspect's] life"[485] is revealed once the officer discovers that the suspect likely has a serious gambling problem. But that discovery is inevitable once the officer is able to freely aggregate the above information. The two-track approach therefore focuses on limiting the utility of aggregated material. Under the two-track approach, an officer may not freely aggregate any information he wishes. For example, a suspect's location over the past few weeks may be logged in a mass surveillance database, but the officer may not search the database without a warrant. A suspect's DNA or urine sample may exist at the police station, but without a warrant, an officer may not run any test he chooses to learn about the suspect from her biological material. Sensitive information is still collected, but individual officers are stopped from aggregating it, so the "intimate picture of [the suspect's] life"[486] is not discovered without a warrant.

To summarize the two-track approach: When the Court has the ability to prohibit an antecedent collection, the Court should regulate use by making it the determinative factor in deciding whether the antecedent collection constituted a reasonable search or seizure. When the Court does not have the ability to prohibit an antecedent collection, it should analyze the use as an independent search that must be reasonable on its own terms. This two-track approach could capture a wide range of uses, so that the Court would be better equipped to take on the challenges posed by modern technology.

2. When Should the Court Apply Use Restrictions?

The above discussion raises several questions: When should the Supreme Court apply use restrictions? When is a discovery sufficiently revealing such that use restrictions are justified? Should every investigative technique be potentially subject to use restrictions?

As discussed in Part III, use restrictions are largely needed now because of emerging technologies that enable novel uses of old collection methods.

---

484 Orin Kerr describes the Fourth Amendment as being based on a "sequential approach," wherein each individual step taken by a state actor is separately analyzed in sequence under the Fourth Amendment. Kerr, *supra* note 458, at 315–16.

485 United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

486 *Id.*

Therefore, revisiting every existing use of collected material is neither necessary nor helpful. The two-track approach is better in part because it can be layered onto existing Fourth Amendment doctrines without upending any case law. Use restrictions should only be applied when (1) the use at issue is novel or surprising, and (2) the use, rather than the collection, is driving the Court's Fourth Amendment concerns.

The first requirement allows current police practices and Fourth Amendment doctrines to mostly stay intact. It would be confusing for police officers and defense attorneys alike if every existing police practice could be challenged under the two-track approach. There are current uses that may be somewhat questionable, but they have the blessing of time. While collecting a suspect's discarded cigarette and then using it to compare the suspect's DNA on the cigarette to the DNA found at a crime scene might have been novel or surprising in the past, it has been permitted by the courts for years.[487] Therefore, such a use should not be challenged under the two-track approach. However, if an abandoned DNA sample like this were used to look for genetic markers linked to aggression, and that individual was closely monitored as a suspect for future assaults, then the Court should be able to restrict such novel use of abandoned DNA.

Surprising uses must also be subject to a use-restriction analysis. There is nothing novel about state actors' sharing information with law enforcement, but depending on the context, it may be quite surprising, and it could violate an individual's reasonable expectation of privacy, as the Court found in *Ferguson*.[488] Relatedly, it would be difficult to characterize the simple act of retaining data as "novel." However, if a police department retained all of its video footage of certain neighborhoods indefinitely, just in case it ever wanted to trace the habits of certain individuals, it would surprise a public that is still taken aback by indiscriminate long-term surveillance.[489]

This would not be the first time the Supreme Court has drawn the line for Fourth Amendment protections based on a practice's novelty or surprise. In *Kyllo*, the Court held that police officers need a warrant to intrude on a constitutionally protected area if they utilize "sense-enhancing technology" that is "not in general public use."[490] The Court could have specified that the

---

487 Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 865, 884 (2006) (arguing for the regulation of the collection and testing of "abandoned" DNA by police, such as DNA left behind on a cigarette or coffee cup); Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445, 447 (2013) (noting that "[s]urreptitious DNA harvesting by the police" has been unregulated by the courts for years).

488 Ferguson v. City of Charleston, 532 U.S. 67, 86 (2001).

489 There was a public outcry when users discovered Uber was tracking them for just five extra minutes after their rides ended. *Uber to End Post-Trip Tracking of Riders as Part of Privacy Push*, CNBC (Aug. 29, 2017, 1:44 AM), https://www.cnbc.com/2017/08/29/uber-to-end-post-trip-tracking-of-riders-as-part-of-privacy-push.html.

490 Kyllo v. United States, 533 U.S. 27, 34 (2001).

technology had to be novel, rather than "not in general public use."[491] It would have been a less ambiguous standard and potentially less subject to criticism.[492] However, it would have also been more limited. The Court's formulation allowed it to reach technology that was not necessarily new but that would surprise people if used against them.

This element of surprise also resonates with *Katz*, which is based on individuals' and society's reasonable expectations.[493] Generically, a surprise is something that violates expectations.[494] If one follows Justice Alito's suggestion in *Jones* that individuals may have reasonable expectations about what police officers may do,[495] then a "surprising" use would be one that violates these reasonable expectations. A surprising use, therefore, may be impermissible under the Fourth Amendment.

However, not every surprising or novel use will require use restrictions. The second prerequisite for applying the two-track approach should be that a specific use, rather than an instance of collection, is driving the Court's Fourth Amendment concerns. For example, imagine a novel collection and a novel use: a public elementary school decides to collect retinal scans of all children so that they can use a retinal scanner to restrict access to the school (perhaps it saves money to replace the security guard with a machine). The use would not drive the Court's concern here; the mandatory scanning and retention of all children's immutable, identifiable biological characteristics would be the far more concerning activity. Therefore, in such a case the Court would not need to engage with the two-track approach and could simply ban the collection outright by applying *Katz* to the retinal scans.[496]

There are multiple advantages to only applying use restrictions when a novel or surprising use is driving the Court's Fourth Amendment concerns. First, it simply is more efficient to only engage with a particular standard if that standard is necessary to resolve the case at hand. Given that many cases hinge on collection alone, it simply is not necessary to explore use restrictions much of the time. Second, as noted above, these two perquisites would limit the number of uses that could be challenged under the two-track approach to a manageable amount, such that Fourth Amendment case law and current

---

491 *Id.*

492 The dissenters in *Kyllo* and academics have attacked the "not in general public use" standard for being too vague and allowing privacy protections to erode over time as technology becomes more invasive. *Id.* at 47 (Stevens, J., dissenting); *see* Heather K. McShain, *Not Quite Bradbury's* Fahrenheit 451*: The Uncertain Future of Sense-Enhancing Technology in the Aftermath of* United States v. Kyllo, 105 W. VA. L. REV. 1, 39–40 (2002). *But see* Marc Jonathan Blitz et al., *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49, 70–71 (2015) (defending the Court's standard).

493 *See* Katz v. United States, 389 U.S. 347, 359 (1967).

494 *Expectancy Violations Theory*, CHANGING MINDS, http://changingminds.org/explanations/theories/expectancy_violations.htm (last visited Jan. 21, 2018).

495 *See supra* Part III.

496 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (describing the Fourth Amendment protection test as "first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

police practices would not be thrown into disarray. Many police departments are fortunately already accustomed to having use restrictions on new technology.[497] Such restrictions may be self-imposed or imposed on them by a legislature.[498] In either case, officers understand that there are restrictions on how they may utilize the new technology. If the Supreme Court and lower courts imposed constitutional use restrictions on new technologies, it would bring a desirable level of nationwide uniformity so that people's civil liberties did not hinge on whether anyone in a given community happened to hear about a new surveillance technology before the local police department acquired and started using it.[499]

Only utilizing use restrictions when (1) the use at issue is novel or surprising and (2) the use, rather than the collection, is the primary reason for the Court's concern would have the advantage of not overly limiting the number of uses the Court could restrict. For example, in the realm of cell phones, *Riley* now dictates that officers may not search a phone incident to arrest.[500] However, what about new "textalyzer" technology that could allow a cell phone to be searched solely for the purpose of showing when the user was last texting, using an app, or browsing the web?[501] Such technology would be extremely useful for immediately determining whether a driver was illegally using her phone at the time of a crash, and it would not otherwise reveal any personal information about the driver. Under *Riley*, a textalyzer ostensibly

---

497 *See, e.g.*, FLA. STAT. §§ 934.50(3)(a), 934.50(4)(b)–(c) (2017) (prohibiting law enforcement officers from using drones except in certain emergency circumstances or when a search warrant has been obtained); Francescani, *supra* note 327 (requiring police destroy surveillance video after thirty days, citing city privacy guidelines).

498 For example, Florida's legislature prohibited law enforcement officers from warrantlessly using drones except in certain emergency situations, and the NYPD's own guidelines for its Domain Awareness System mandate that officers destroy footage over thirty days old. FLA. STAT. §§ 934.50(3)(a), 934.50(4)(c) (2017); Francescani, *supra* note 327.

499 For example, the City of Kyle, Texas had approved a program where their police department would get to use a private company's automated license plate readers for free to find drivers with outstanding fines. Dave Maass, *A Texas City Rescinds "No Cost" License Plate Reader Deal for Being "Big-Brotherish"*, ELEC. FRONTIER FOUND., DEEPLINK BLOG (Feb. 25, 2016), https://www.eff.org/deeplinks/2016/02/texas-city-rescinds-license-plate-reader-contract-being-big-brotherish. Police officers had credit card readers put into their cars so they could find drivers with fines, charge them on the spot, and charge them an extra 25 percent to pay for the technology. *Id.* It was not until the Electronic Frontier Foundation and the Texas Civil Rights Project called attention to the program that the City Council belatedly pulled out of the arrangement. *Id.* Other communities have not had any local governmental response to identical programs, despite some belated concerns. *See, e.g.*, Eric Dexheimer, *Local Police Use of Vast License Plate Database Raises Privacy Concern*, AUSTIN AM.-STATESMAN (Feb. 18, 2016, 3:28 PM), http://www.mystatesman.com/news/local-police-use-vast-license-plate-database-raises-privacy-concern/HXB5UL1BYyUlUOyhnFalOI/.

500 Riley v. California, 134 S. Ct. 2473, 2495 (2014).

501 *See* Kelly Wallace, *Driving While Distracted: Is the Textalyzer the New Breathalyzer?*, CNN (Sept. 2, 2016, 2:03 PM), http://www.cnn.com/2016/09/02/health/distracted-driving-textalyzer/index.html.

could not be used for such a search incident to arrest.[502] But would the Court really want to prohibit such a use? Given its case law on dog sniffs and field drug tests, probably not.[503] Fortunately, the requirement that use restrictions only be applied when a use is novel or surprising would not prevent the Court from revisiting *Riley* and periodically creating new rules for cell phone searches and other novel areas of law as technology progresses.

3. The Effects of Imposing Use Restrictions.

In advocating for a new doctrine, it is important to consider what effects that doctrine would have beyond the case law. This subpart briefly considers what the impact would be on affected individuals and institutions if the Court openly imposed use restrictions.

a. *Effects on Lower Courts.*

Courts may often be overwhelmed by the prospect of law enforcement use of modern technologies. Judges are not known for being especially tech-savvy, and police departments are not always forthcoming about the details of their new technologies.[504] When the implications of a given technology or police practice are unclear, it puts judges in a difficult position. They can either require officers to always get a warrant to collect material with the new technology, or they can give officers free reign to collect as much material as they like, while the judges know that their own knowledge and control over how the collected material will be used is virtually nil.

The latter is a frustrating place to be. A handful of magistrate judges have sought to bridge the gap between the two choices by imposing use restrictions in the warrants they sign, but the legality of these restrictions is somewhat dubious.[505] If use restrictions became the law of the land, these magistrates would be able to more finely control officers' behavior as they

---

502 *See Riley*, 134 S. Ct. at 2493–94 (holding that a warrant is required when a cell phone is seized incident to arrest, subject to certain established case-specific exceptions, such as exigent circumstances).

503 *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984) ("A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy."); United States v. Place, 462 U.S. 696, 707 (1983) (holding that a sniff performed by a dog trained to sniff for drugs was not a search because the act was "so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure").

504 Prosecutors have offered defendants plea bargains rather than reveal the specifics of new technologies they use. Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015), http://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html.

505 *See* Ann E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), https://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html?utm_term=.ae44bfc835f0.

see fit. Courts would have more options for weighing in on police behavior. The same cost would exist as exists any time a new doctrine is introduced, in that lower courts would need to flesh out the parameters of what it means to impose use restrictions and develop a coherent body of case law around them. However, the degree of control the lower courts would get in this process would be a real benefit.

Courts could validate certain collection methods without having to simultaneously sign off on every current and future use of the collected material. They could revisit the unforeseen consequences of new technologies more readily, as defendants could bring cases each time a new or surprising use arose. This would take pressure off lower courts, which otherwise may only have one chance to judge a new technology. Courts would be empowered to assert some control over how technology affects individuals' Fourth Amendment rights and how the Fourth Amendment can stay relevant in a time of rapidly evolving technologies. At the same time, if a court had no concerns about a given use or technology, then use restrictions would not need to play any part in the court's Fourth Amendment analysis, avoiding unnecessary legal analysis.

b. *Effects on Law Enforcement.*

Legal doctrines affect what methods law enforcement officers use.[506] Officers want to stay on the right side of the law so that a court does not exclude the evidence collected.[507] Therefore, if a practice becomes more restricted or uncertain, officers will focus their energies on relatively unrestricted practices certain to withstand legal scrutiny.

Use restrictions can channel officers' efforts away from mass surveillance. If a warrant were required to track a suspect's GPS coordinates for an extended period of time (as the *Jones* shadow majority suggested and the *Carpenter* Court held in the context of third party–held records),[508] officers would likely use other means to focus on a specific time frame, so they could avoid getting a warrant. If officers knew a court would likely decide a warrant is needed to broadly search a law enforcement surveillance database, officers might use a more targeted method to find suspects instead of scanning through hundreds of people's records. More generally, officers would be encouraged to be more thoughtful and more circumspect about how they use the material they collect to make sure they do not accidentally jeopardize the admissibility of the evidence they uncover.

---

506 *See* Ken Wallentine, *PoliceOne Analysis: 12 Supreme Court Cases Affecting Cops*, POLICEONE.COM (Nov. 11, 2009), https://www.policeone.com/legal/articles/1964272-PoliceOne-Analysis-12-Supreme-Court-cases-affecting-cops/.

507 *See* Davis v. United States, 564 U.S. 229, 231–32 (2011) (explaining that the exclusionary rule is "a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation").

508 *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); United States v. Jones, 565 U.S. 400, 430–31 (2012) (Alito, J., concurring in judgment).

Not all of the effects of use restrictions are desirable for law enforcement. It may be disheartening for officers to see guilty men go free because evidence is excluded based on a use restriction. This may be particularly true if use restrictions are seen as less legitimate or more confusing than other doctrines that trigger the exclusionary rule. Additionally, use restrictions may force officers to use more onerous police practices to learn information about suspects. If a city is covered in surveillance cameras, but a warrant is required to look up a given person's whereabouts, the officer will have to resort to tailing the suspect in person if he lacks probable cause for a warrant. This is preferable from the perspective of avoiding casual mass surveillance, but it is a real cost for police officers and police departments to absorb.

c. *Effects on the Public.*

The public worries about mass surveillance.[509] Technology changes more rapidly than many people can keep up with, and popular TV shows like *CSI* can make law enforcement officers seem almost superhuman.[510] If the Supreme Court openly imposed use restrictions, the public may be reassured that there are some limits on how governments may deploy surveillance technology. Though most people do not closely follow developments in Fourth Amendment case law, they do care about what their local police departments may do.[511] There have been several recent instances where communities were unexpectedly vocal about wanting to restrict what technology their police departments could acquire, and how they could use it.[512] Most people do not anticipate ever becoming suspects in criminal investigations, but they might imagine themselves being swept up in a broader surveillance dragnet.[513] A Supreme Court holding that courts can restrict how police departments use

509 *See* Jeff Guo, *New Study: Snowden's Disclosures About NSA Spying Had a Scary Effect on Free Speech*, WASH. POST (Apr. 27, 2016), https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/?utm_term=.0c4123a4508f.

510 *See How to Become a CSI*, INT'L CRIME SCENE INVESTIGATORS ASS'N, http://www.icsia.org/how-to-become-a-csi/ (last visited Jan. 18, 2018).

511 *See* Emily Ekins, *Policing in America: Understanding Public Attitudes Toward the Police. Results from a National Survey*, CATO INSTITUTE (Dec. 7, 2016), https://www.cato.org/survey-reports/policing-america.

512 *See* Selena Larson, *Communities Call for More Control Over Police Surveillance*, CNN (Feb. 17, 2017, 1:32 PM), http://money.cnn.com/2017/02/07/technology/cop-surveillance-aclu-santa-clara-bart/index.html; Elizabeth Weise, *Amazon's Controversial Facial Recognition Program Dropped by City of Orlando*, USA TODAY (June 25, 2018, 5:32 PM), https://www.usatoday.com/story/tech/talkingtech/2018/06/25/amazons-controversial-facial-recognition-program-dropped-city-orlando/732090002/.

513 *See generally* THE SENTENCING PROJECT, HALF IN TEN, AMERICANS WITH CRIMINAL RECORDS 1 (2015), https://www.sentencingproject.org/wp-content/uploads/2015/11/Americans-with-Criminal-Records-Poverty-and-Opportunity-Profile.pdf (reporting that only thirty percent of Americans have criminal records); *Everyone Is Under Surveillance Now, Says Whistleblower Edward Snowden*, THE GUARDIAN (May 3, 2014, 1:27 AM), https://www.theguardian.com/world/2014/may/03/everyone-is-under-surveillance-now-says-whistleblower-edward-snowden.

surveillance technologies could provide significant reassurance to citizens concerned about surveillance in their communities.

There is a cost to turning law enforcement away from certain novel tools. Officers may sometimes use more intrusive means to investigate individuals than they would in a world without use restrictions. For example, imagine an officer could get a general sense of what a suspect is like either by running an algorithm that draws conclusions based on the suspect's social media postings around the web, or by talking to his friends and relatives. Both the officer and the suspect might prefer the officer take the easier route of running the algorithm, rather than bothering the suspect's friends and relatives and alerting them that he is a suspect in a criminal investigation. The algorithm may not be available if a court decides that officers need a warrant to run any kind of algorithm purporting to psychoanalyze an individual, as with the Chicago hot list. Society as a whole would gain from knowing that its police officers are not secretly running algorithms judging people at will, and potentially sorting them into lists for disparate treatment based on a secret algorithm. But individuals who are sufficiently of interest to the police would suffer by being subjected to a more intrusive investigation than would otherwise occur. Under this rubric, many more people would see privacy gains than would suffer intrusive surveillance. But the losses for the individual singled out for investigation would be significantly greater than the privacy gains for any one uninvestigated individual.

Many of the scariest uses of modern technology have not yet been realized, but they exist within the public's imagination. It does not appear that any police department has a pervasive system of cameras equipped with facial recognition technology.[514] Pre-crime programs are not in the works, even in Chicago. But trust in law enforcement institutions is low,[515] and the idea that the NSA is spying on all of us has become a running joke since the Edward Snowden revelations.[516] By openly imposing use restrictions, the Court could reassure the public that at least one branch of government is protecting people's privacy, and we are not necessarily headed towards any kind of dystopian authoritarian state.

---

514 *See* Kofman, *supra* note 323 (reporting that while some police departments are using both cameras and facial recognition, these systems are not yet paired in real-time systems).

515 *See* Bill Bishop, *Americans Have Lost Faith in Institutions. That's Not Because of Trump or 'Fake News.,'* WASH. POST, (Mar. 3, 2017), https://www.washingtonpost.com/posteverything/wp/2017/03/03/americans-have-lost-faith-in-institutions-thats-not-because-of-trump-or-fake-news/?utm_term=.46b28317d70c.

516 *See, e.g.*, Kellen Beck, *Alexa Does Not Like When You Ask Her About the NSA*, MASHABLE (June 29, 2016), http://mashable.com/2016/06/29/amazon-alexa-nsa/#edwyuNshe5qV. *But see* Bob Litt, *Privacy, Technology and National Security: An Overview of National Intelligence Collection* (July 19, 2013), https://www.lawfareblog.com/odni-gc-bob-litt-speaking-brookings (providing a soberer take on how members of the intelligence community view their legal obligations).

4. Enforcing Use Restrictions.

When law enforcement officers wish to collect material, they often need to do so in public, or they need to acquire material from a party who will not give up the material absent a warrant.[517] When a law enforcement officer wishes to use collected material, the officer is usually acting in private and does not need to interact with any recalcitrant parties.[518] Use restrictions are therefore potentially more difficult to enforce than collection restrictions. As Kiel Brennan-Marquez and Stephen Henderson have argued, "closed-door policing," in which there is no one watching over the officer in real time, is a legitimate concern.[519]

However, there are at least three mechanisms society can rely on to enforce use restrictions. The first is simply the professionalism of American law enforcement officers. Our law enforcement system is incredibly rule heavy,[520] and officers can get into serious trouble for breaking the rules.[521] Second, if law enforcement officers want prosecutors to be able to use the evidence they produce, they cannot act in ways that will trigger the exclusionary rule.[522] The exclusionary rule would apply to use restrictions just as it applies to most Fourth Amendment doctrines. If a use restriction prohibited officers from running familial DNA searches on arrestees' DNA,[523] but an officer nevertheless did so and discovered an arrestee's brother was the likely perpetrator in a cold case, the first questions a defense lawyer would ask would be "why did you suddenly reopen this cold case?" and "why did you immediately suspect my client?" The officer's unconstitutional actions would come to light, and the DNA match and all the evidence that flowed from it would be excluded. Even if one assumes the officer would deviously concoct a story for how he happened to reopen the cold case and came to suspect the brother, there would still likely be a record of the DNA test. This

---

517 *See* Timothy Roufa, *A Day in the Life of a Police Detective*, THE BALANCE (Oct. 29, 2017), https://www.thebalance.com/a-day-in-the-life-of-a-police-detective-974874.

518 *See id.*

519 *See generally* Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1, 24–25 (2018) (discussing "closed-door" policing).

520 *See, e.g.*, *Read the Entire Current NYPD Patrol Guide Online*, HARVIS & FETT (Nov. 15, 2014), http://www.civilrights.nyc/blog/2014/11/15/read-the-entire-current-nypd-patrol-guide-online (containing over 2,000 pages of instructions for all New York City police officers in a variety of situations).

521 *See, e.g.*, U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN. EVALUATION & INSPECTIONS DIV., REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S DISCIPLINARY SYSTEM i–ii (May 2009) (outlining the FBI's detailed system for investigating and disciplining its own employees).

522 *See* Davis v. United States, 564 U.S. 229, 231–32 (2011) (explaining that the exclusionary rule is "a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation").

523 Familial DNA searches can determine if an individual's DNA is likely closely related to another, unidentified DNA sample. *See* Eli Rosenberg, *Family DNA Searches Seen as Crime-Solving Tool, and Intrusion on Rights*, N.Y. TIMES (Jan. 27, 2017), https://www.nytimes.com/2017/01/27/nyregion/familial-dna-searching-karina-vetrano.html?_r=0.

leads to the third mechanism—that since many use restrictions would be attached to new technologies, these technologies could be designed to incorporate use restrictions. Businesses have had audit trails for years tracking what each user does on a business's system.[524] Tracking each user's activity deters employees and contractors from wantonly looking up whomever they might be curious about, because they know their actions will leave a trail. Similarly, police officers could be deterred from misusing surveillance systems if all their actions on the system were recorded, or if certain actions required a supervisor's signoff and credentials. [525]

These methods are not foolproof, but they go a long way towards making use restrictions more than a paper tiger. One additional level of protection could come from organizations like the ACLU. The ACLU has previously filed suits against law enforcement where it believes there has been a pattern of constitutional violations.[526] In *Raza v. City of New York*,[527] the ACLU led a challenge against the New York City Police Department's surveillance of Muslims following 9/11.[528] The complaint alleged violations of the First and Fourteenth Amendments—specifically, the right to freely exercise religion, the Establishment Clause, and the Equal Protection Clause.[529] The ACLU was able to reach a settlement that altered the NYPD's practices and ensured some level of civilian review.[530] If the ACLU or another organization believed that a police department systematically used material in a way that violated the Fourth Amendment, it would have the power to sue and potentially alter the way the department used collected material in every case going forward.

There will always be the potential for law enforcement officers to misuse material in secret. For example, a police department could have a secret unconstitutional version of Chicago's hot list and alter its policing based on the list. However, if the alteration is subtle enough that it never comes to light via a defense attorney suspecting his client was unfairly targeted, or an organization like the ACLU picking up on it, then the altered behavior and accompanying harm may simply not be that great. It would likely be easier to violate use restrictions than collection restrictions, but there are sufficient

---

524 *See* Arup Nanda, *Managing Audit Trails*, ORACLE MAGAZINE (Nov./Dec. 2010), http://www.oracle.com/technetwork/issue-archive/2010/10-nov/o60security-176069.html.

525 *See* ABA STANDARDS FOR CRIMINAL JUSTICE, *supra* note 463, at § 25-6.1(b)(i), cmt. (requiring such audit logs).

526 *See, e.g.*, *Raza v. City of New York – Legal Challenge to NYPD Muslim Surveillance Program*, ACLU (Aug. 3, 2017), https://www.aclu.org/cases/raza-v-city-new-york-legal-challenge-nypd-muslim-surveillance-program; *The Right to Keep Personal Data Private: Carpenter v. U.S.*, ACLU (Sept. 15, 2017, 11:00 AM), https://www.aclu.org/blog/privacy-technology/location-tracking/right-keep-personal-data-private-carpenter-v-us.

527 998 F. Supp. 2d 70 (E.D.N.Y. 2013).

528 *Id.* at 73.

529 *Id.*

530 *Second and Final Judge Approves Settlement on NYPD Muslim Surveillance*, ACLU (Mar. 21, 2017), https://www.aclu.org/news/second-and-final-judge-approves-settlement-nypd-muslim-surveillance.

enforcement mechanisms to make use restrictions constitutional protections worth having.

CONCLUSION

We live in an age where we all leave behind a path of digital breadcrumbs.[531] A man walks outside past a security camera, he swipes his credit card for a free-trade coffee, he "likes" a couple of posts on Facebook as he sips his coffee. Any individual action is insignificant. Aggregated, these and other actions form "an intimate picture of his life."[532]

The Court must address the fact that the prevalence of digital breadcrumbs, cheap data storage, and advances in machine learning are on the edge of transforming our relationship with law enforcement. Police departments, tasked to defend us against crime and terrorism, will use new technologies in any way they can to protect us. That means they will push up to the boundaries of the Fourth Amendment. The Court has made it clear that it intends to push back.[533]

The Court has already dealt with the necessity for use restrictions in cases that do not hinge on modern technology. In *Ferguson*, the Court created a use restriction without announcing what it was doing.[534] In *NASA*, the Court assumed without deciding that a disclosure-related use restriction exists.[535] These are not plausible approaches going forward. Neither is the mosaic theory, which speaks to the heart of the problem but fails to offer a workable judicial rule.

Part of the Fourth Amendment's strength is its ability to support a coherent body of case law. Fourth Amendment law may be messy and fact specific, but it provides a set of rules for state actors to follow. That set of rules protects us and our everyday "privacies of life."[536] To keep the Fourth Amendment strong and the case law coherent, the Court should hold its head up high and openly impose use restrictions.

---

531 *See* Yuki Noguchi, *Following Digital Breadcrumbs to 'Big-Data' Gold*, NPR (Nov. 29, 2011, 3:34 AM), http://www.npr.org/2011/11/29/142521910/the-digital-breadcrumbs-that-lead-to-big-data.

532 United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

533 *See* NASA v. Nelson, 562 U.S. 134, 158 (2011); *Maynard*, 615 F.3d at 562; Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001).

534 *See Ferguson*, 532 U.S. at 84–85.

535 *See NASA*, 562 U.S. at 158.

536 Boyd v. United States, 116 U.S. 616, 630 (1886).