

GOVERNMENT ANALYSIS OF SHED DNA IS A SEARCH UNDER THE FOURTH AMENDMENT

*Tracey Maclin**

I. INTRODUCTION	287
II. DOES ANALYSIS OF SHED OR COVERTLY OBTAINED DNA CONSTITUTE A SEARCH?.....	291
III. TENSION BETWEEN CASES.....	298
IV. IMPLICATIONS OF LEAVING THE ANALYSIS OF ABANDONED DNA UNREGULATED BY THE FOURTH AMENDMENT	307
V. CONCLUSION.....	311

I. INTRODUCTION

The Fourth Amendment in the 21st Century was the subject of the 2015 Texas Tech School of Law Criminal Law Symposium. My panel considered DNA and the Fourth Amendment—a subject that has generated abundant, thoughtful scholarship and genuine controversy among jurists, politicians, academics, and the public at large.¹ Any discussion about DNA and search and seizure law must consider the Supreme Court’s 2013 ruling in *Maryland v. King*.²

King addressed whether a state could forcibly obtain and analyze a DNA sample from someone arrested for a serious felony.³ During the oral argument in *King*, Justice Kennedy asked King’s counsel a series of questions focusing on whether law enforcement officials had a legitimate interest in knowing whether an arrestee had committed other crimes.⁴ While counsel

* Professor of Law, Boston University School of Law. I want to thank Elizabeth Parker and Josh Butera for their excellent research and editing assistance.

1. My understanding of this area of the law has been enhanced by the outstanding legal scholarship of Professors Erin Murphy and David H. Kaye.

2. *Maryland v. King*, 133 S. Ct. 1958 (2013).

3. *See id.* at 1966.

4. Transcript of Oral Argument at 41–43, *King*, 133 S. Ct. 1958 (No. 12-207), 2013 WL 1842092. Justice Kennedy posed the following questions:

[A] person has been arrested for a felony and is in custody, do the police—does the justice system have an interest in knowing whether that person committed other crimes?

.....

My question is whether or not the police, who have John Doe in custody for a felony, have an interest in knowing, at the outset or within a few weeks’ time, whether or not that person has committed other crimes?

.....

And my—my question is, do they have an interest—a legitimate interest in knowing if that person has committed other crimes?

for King did not provide the answers Justice Kennedy sought, Justice Kennedy eventually answered his own questions in an opinion for a majority of the Court.⁵ Police officials do have a legitimate interest in knowing whether someone arrested for a serious crime has committed other offenses.⁶ In a 5–4 ruling, *King* held that when the police have probable cause to arrest for a serious offense, “taking and analyzing a cheek swab of the arrestee’s DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.”⁷

Of course, Justice Kennedy’s inquiries on the state’s interest in knowing whether someone had committed other crimes were posed in a context in which the police made a lawful arrest and utilized means that have a negligible impact on the bodily integrity of the arrestee.⁸ Justice Kennedy’s queries, however, prompt related questions about DNA as an investigative tool and the Fourth Amendment rights of persons for whom the police do not have evidence to detain or arrest.

For example, does a state have a legitimate interest in knowing whether citizens have committed unsolved crimes? If negligible means can be utilized to obtain DNA samples from individuals, does the state have a legitimate interest in collecting and analyzing those samples to determine whether a person has committed crimes in the past, or to connect that person to a crime committed sometime in the future? Professor Arnold Loewy’s provocative Article for this Symposium offers a proposal along these lines for the universal collection of DNA samples to use for law enforcement purposes.⁹ Finally, what if a state can obtain a DNA sample without a bodily intrusion and without the knowledge of the person; does the state have a legitimate interest in collecting, testing, and storing those samples?

Id.

5. *King*, 133 S. Ct. at 1965–80.

6. *Id.* at 1977.

7. *Id.* at 1980.

8. *Id.* at 1969 (describing a buccal swab to obtain a DNA sample as “a far more gentle process than a venipuncture to draw blood,” and noting that the “fact tha[t] an intrusion is negligible is of central relevance to determining reasonableness, although it is still a search as the law defines that term”).

9. Arnold H. Loewy, *A Proposal for the Universal Collection of DNA*, 48 TEX. TECH. L. REV. 261 (2015). Others have called for similar types of universal DNA collection from the population. See D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413; Eric Posner, *The Mother of DNA Databases*, SLATE (Mar. 5, 2013, 12:04 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2013/03/dna_at_the_supreme_court_the_case_for_a_universal_database.html.

With a minimal privacy intrusion, [DNA testing] can provide accurate evidence that leads to convictions. If we really care about rights, we should mandate DNA testing, and not only of arrestees, but of everyone. A universal DNA database would greatly increase the number of convictions—vindicating the rights of rape victims and protecting others from serial rapists. . . . Such a database would greatly reduce the incidence of false convictions, thus protecting the rights of innocent people who are wrongly accused.

Posner, *supra*.

The answer to the third question—whether a state has a legitimate interest in covertly collecting and analyzing someone’s DNA sample—seems almost too easy. I believe this is the question judges intuitively asked themselves when confronted with a Fourth Amendment claim in the so-called abandoned DNA cases, although these cases have been nominally decided by asking whether the individual has an expectation of privacy in the furtively secured DNA sample.¹⁰ Of course, the state has a legitimate interest in collecting and testing DNA surreptitiously obtained from individuals. Cases are now legendary where police have successfully resolved, sometimes decades-old, otherwise unsolvable murders and other serious crimes by covertly and unobtrusively obtaining a DNA sample from someone who the police did not originally have sufficient cause to arrest or detain.¹¹ The results in these cases make plain that the state does have a legitimate interest in securing and analyzing DNA obtained from individuals whom the Constitution bars the police from detaining. That is why courts have been nearly unanimous in rejecting Fourth Amendment challenges to the collection and analysis of DNA samples obtained without force or coercion, and allowing the admission of that analysis in criminal prosecutions.¹²

10. For thoughtful analysis of this issue, see Elizabeth E. Joh, *Reclaiming “Abandoned” DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006) and Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445 (2013). Throughout this Article, I use the terms *abandoned* or *shed* DNA interchangeably. As Professor LaFave explains, under property law concepts, when a person is said to have “abandoned” an item, that use of the term normally means that the person has voluntarily, intentionally, and unconditionally surrendered his interest in the item. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(b), at 878 (5th ed. 2012). That narrow and more protective definition of abandonment does not apply in the Fourth Amendment context. *See id.* Under the Fourth Amendment, courts focus on whether a person, in abandoning or discarding an item, has relinquished his or her reasonable expectation of privacy in the item. *Id.* “The fundamental question is whether the relinquishment occurred under circumstances indicating he retained no justified expectation of privacy in the object.” *Id.* Professor Joh defines abandoned DNA as follows: “‘Abandoned DNA’ is any amount of human tissue capable of DNA analysis and separated from a targeted individual’s person inadvertently or involuntarily, but not by police coercion.” Joh, *supra* at 859 (footnote omitted).

11. *See* Joh, *supra* note 10, at 860–62 (providing cases).

12. *Id.* at 868 (“No court has held police collection of abandoned DNA to be illegal. Once DNA is considered abandoned or knowingly exposed, the Fourth Amendment does not apply at all.”); Scherr, *supra* note 10, at 454 (“Courts have uniformly rejected Fourth Amendment protection against surreptitious harvesting of out-of-body DNA by the police.”); *see also* LAFAVE, *supra* note 10, at 877–78 (noting cases in which courts have held “that one abandons the hair he has cut off by a barber, the saliva he expectorates onto a public sidewalk[,] leaves on a discarded paper cup, or uses in licking an envelope he then places in the mail, and the excreta he deposits in a hospital bedpan.” (footnotes omitted)). Although she does not discuss biological material specifically, Maureen E. Brady’s article, *The Lost “Effects” of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. (forthcoming 2016), explains that for many lower courts, the public nature of property seized by the police resolves whether a person enjoys Fourth Amendment protection for items left in a location accessible to the public: “the location of the effect is the sole or dominant factor in determining whether an individual has ‘abandoned’ his or her privacy expectations and thus relinquished any claim to Fourth Amendment protection.”

Regarding the results in these cases, Professor Scherr writes that courts have focused narrowly on the “putative suspect’s privacy in the discarded item,” and not “explicitly considered either the person’s privacy rights in the DNA itself or the nature and extent of those genetic-privacy rights.” Scherr, *supra*

The existence of a legitimate state interest, however, does not end the constitutional inquiry when the state seeks to admit DNA evidence in a criminal prosecution. Although the existence of a legitimate interest that is rationally enforced suffices when the state is alleged to have impacted non-fundamental rights, such an interest should not override a Fourth Amendment right, which is a fundamental and foundational liberty.¹³ When utilizing abandoned or shed DNA for criminal investigative purposes, there are two state actions that arguably trigger Fourth Amendment protection.¹⁴ First, the collection of the biological material that contains a person's DNA might be considered a search under the Amendment.¹⁵ Courts, however, have rejected this argument.¹⁶ To date, judges have concluded that the individual "abandoned the item upon or in which the DNA-laden cells were found," and thus, under Fourth Amendment law, retained "no expectation of privacy in the item or that which it was in or on."¹⁷

note 10, at 454. According to Scherr, a proper reasonable expectation of privacy inquiry would consider the property status of the shed DNA, as well as "the information which that DNA may contain," and the "individual's attitude towards that DNA and its contents." *Id.* at 464. The judiciary's focus on the property status of abandoned DNA is another example of what Professor Orin Kerr has described as a "'loose' version of real property law" that controls whether a police intrusion invades a reasonable expectation of privacy. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004). "Under these precedents, a 'reasonable expectation of privacy' is not the same as the privacy that a reasonable person would expect. Instead, it acts as a term of art tied largely to traditional property law concepts." *Id.* Although his article does not discuss the shed DNA cases, Professor Kerr's thesis accurately describes the results of these cases: "Most existing Fourth Amendment rules in new technologies are based heavily on property law concepts, and as a result offer only relatively modest privacy protection in new technologies." *Id.* at 838. Thus, it is no surprise that lower courts have unanimously ruled that the collection of shed DNA samples does not infringe upon a target's privacy expectation; the government has a legitimate interest in obtaining biological samples that have been abandoned by a target. These results reflect "a relatively humble and deferential judicial attitude." *Id.*

13. See *Harris v. United States*, 331 U.S. 145, 163 (1947) (Frankfurter, J., dissenting), *overruled in part* by *Chimel v. California*, 395 U.S. 752 (1969). Justice Felix Frankfurter and Professor Yale Kamisar have nicely described why the Fourth Amendment is a fundamental and foundational freedom. See *id.* ("How can there be freedom of thought or freedom of speech or freedom of religion, if the police can, without warrant, search your house and mine from garret to cellar merely because they are executing a warrant of arrest?"); Yale Kamisar, *The Fourth Amendment and Its Exclusionary Rule*, CHAMPION, Sept.–Oct. 1991, at 2 ("What good is freedom of speech or freedom of religion or any other freedom if law enforcement officers have unfettered power to violate a person's privacy and liberty when he sits in his home or drives his car or walks the streets?").

14. Cf. *State v. Medina*, 102 A.3d 661, 667 (Vt. 2014) (noting that, in the course of addressing the constitutionality of Vermont's law authorizing the collection of DNA from those arraigned on felony charges, the initial taking of the DNA sample constitutes a search under the Vermont constitution, "and the subsequent analysis, storage, and searching of the DNA profile" is a second search "upon personal security that merit[s] scrutiny" under the state constitution (quoting *State v. Martin*, 955 A.2d 1144, 1151 (Vt. 2008))).

15. See Scherr, *supra* note 10, at 487 (explaining that "[i]f 'entry' of the physical boundaries of the body occurs when [the government] enters [the biological sample] to obtain what will become the alphanumeric identification tag used in forensic DNA analysis, then it is an intrusion").

16. *Id.* at 454.

17. *Id.*

Second, the analysis of the DNA sample might trigger Fourth Amendment safeguards. This second issue—whether the Fourth Amendment is implicated when police surreptitiously analyze a citizen’s involuntarily shed DNA—is the topic of this Article. Specifically, Part II discusses whether analysis of abandoned DNA constitutes a search under the Fourth Amendment.

Part III considers a conflict in the Court’s cases when new technology or science gives law enforcement authorities enhanced capabilities to discover information arguably protected by the Fourth Amendment. In some cases, when deciding whether a search occurred, or the reasonableness of a challenged search, what a particular intrusion *actually* reveals matters little; rather, what matters is the *potential* risk to privacy posed by new technology. In other cases, the fact that a particular intrusion has the potential to disclose highly personal data or massive amounts of information is constitutionally irrelevant. The only thing that matters is what the intrusion actually revealed. Finally, Part IV considers the implications of leaving the analysis of shed DNA unregulated by the Fourth Amendment.

II. DOES ANALYSIS OF SHED OR COVERTLY OBTAINED DNA CONSTITUTE A SEARCH?

On April 2, 2006, a woman in Bel Air, Maryland, was raped in her home.¹⁸ The attack occurred very early in the morning. The perpetrator entered the victim’s bedroom, pressed a pillow against her face, and blindfolded her with his t-shirt. “The victim noticed, however, that her attacker was Caucasian, had a medium build, and emanated a ‘metallic scent.’”¹⁹ After the perpetrator fled the scene, the victim contacted the police. Police technicians gathered blood samples found in the bedroom and near the door where the perpetrator had entered. The victim was taken to a hospital, “where she underwent a rape examination, during which a nurse took vaginal and anal swabs,” which disclosed biological material of the rapist.²⁰ These biological samples were analyzed and enabled law enforcement officials to develop a DNA profile of the rapist.

Over the next two years, police obtained consensual DNA samples from nearly twenty persons who might have been involved with the rape. None of those samples matched the DNA found in the victim’s home and taken during the rape examination. In July 2008, the victim told police that she suspected Glenn Raynor was the rapist. Raynor and the victim “had gone to school together, he was the previous owner of the home in which the rape occurred, and his body type matched that of the man who raped her.”²¹ After being

18. Raynor v. State, 99 A.3d 753, 755 (Md. 2014), *cert. denied*, 135 S. Ct. 1509 (2015).

19. *Id.*

20. *Id.*

21. *Id.*

contacted by the police, Raynor agreed to meet with them and talk about the rape. Raynor wore a short-sleeved shirt to the interview, and “repeatedly rubbed his bare arms against the armrests of his chair, and his body carried a metallic odor similar to the odor” described by the victim.²² When the police asked Raynor for a DNA sample, he “responded that he would consent only if the police agreed to destroy the DNA sample after they concluded their investigation of the rape.”²³ When the police refused, Raynor denied the request and the interview ended.

After Raynor left the police station, officers took swabs of the armrests of the chair where Raynor had sat.²⁴ Analysis of those samples showed a match with the DNA profile taken from the rape scene.²⁵ Police then arrested Raynor and obtained his DNA sample via a buccal swab. Subsequent analysis of the DNA from the buccal swab revealed a match to the DNA profile collected from the victim’s home and from the vaginal and anal swabs obtained during the rape examination. Raynor was charged with rape, assault, burglary, and other crimes. At trial, the jury received the DNA analysis; Raynor was convicted of rape and other crimes, and sentenced to one hundred years of imprisonment.²⁶

On appeal, an intermediate appellate court ruled that the Fourth Amendment did not apply to the analysis performed on the DNA samples Raynor left on the chair.²⁷ The court reasoned that the testing of the genetic material produced a DNA profile that was only used for identification purposes and that Raynor had “no objectively reasonable expectation of privacy in the identifying characteristics that could be gleaned from the normal biological residue he left behind.”²⁸

Raynor appealed the ruling to Maryland’s highest court. According to the Court of Appeals of Maryland, the issue was whether police “testing of the identifying loci within . . . DNA material for the purpose of determining whether those loci match that of DNA left at a crime scene constitutes a search under the Fourth Amendment.”²⁹ The Court of Appeals held that analyzing the biological material found on the chair Raynor sat in “is no more

22. *Id.* at 755–56.

23. *Id.* at 756.

24. This was an example of “touch” or “contact” DNA harvesting. See Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1504 (2015). As Professor Jason Kreag explains in a recent article, new technologies have enabled the government “the ability to obtain full forensic DNA profiles from exceedingly small amounts of biological material.” *Id.* According to Professor Kreag, analysts can procure DNA profiles from the skin cells shed when touching objects. *Id.* “For example, shed skin cells can be collected from the handle of a gun, the portion of a torn screen touched by an intruder, a brick used to break a window in a burglary, or the steering wheel of a stolen vehicle.” *Id.*

25. *Raynor*, 99 A.3d at 757.

26. *Id.* at 756.

27. *Id.* at 757.

28. *Id.* (quoting *Raynor v. State*, 29 A.3d 617, 626 (Md. Ct. Spec. App. 2011)).

29. *Id.*

a search for purposes of the Fourth Amendment, than is the testing of fingerprints, or the observation of any other identifying feature revealed to the public—visage, apparent age, body type, skin color.”³⁰ The court dismissed Raynor’s contention that analysis of DNA samples differs from fingerprints because DNA testing has the potential to provide more information about a person.³¹ The possibility that Raynor’s “DNA could have disclosed more intimate information is of no moment in the present case because there is no allegation that the police tested his DNA sample for that purpose.”³²

The result in *Raynor v. State* conflicts with a ruling of the Fourth Circuit, the federal circuit in which Maryland sits.³³ In *United States v. Davis*, the Fourth Circuit ruled that the analysis of a suspect’s DNA sample from clothing, lawfully obtained by the police, was a search.³⁴ The Fourth Circuit explained that “analysis required to obtain a DNA profile . . . generally qualifies as a search, because an individual retains a legitimate expectation of privacy in the information obtained from the testing.”³⁵ *Raynor*, however, thought that *Davis* rested on “a faulty premise,” in light of the logic of *King*—“that DNA analysis limited to the 13 junk loci within a person’s DNA discloses only such information as identifies with near certainty that person as unique.”³⁶

Raynor’s reliance on *King*, that chemical analysis of a DNA sample does not constitute a search, is paradoxical in light of its statement that “[t]he case at bar implicates those questions left unanswered in *King*.”³⁷ On the other hand, it is understandable why Maryland’s highest court cited *King* in rejecting Raynor’s claim.³⁸ First, Justice Kennedy’s opinion in *King* asserts that the processing of a DNA sample does “not intrude on [an arrestee’s]

30. *Id.* at 767.

31. *Id.*

32. *Id.* at 768.

33. See *United States v. Davis*, 690 F.3d 226, 243–46 (4th Cir. 2012). A conflict between “the decision of a [federal] court of appeals and that of the highest court of a state where that conflict concerns a federal question” is an “established reason for the grant of certiorari” by the Supreme Court. STEPHEN M. SHAPIRO ET AL., SUPREME COURT PRACTICE § 4.9, at 259 (10th ed. 2013).

34. *Davis*, 690 F.3d at 243–46.

35. *Id.* at 243–44.

36. *Raynor*, 99 A.3d at 764.

37. *Id.* at 759; see also Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SUR. AM. L. 639, 658 (2014) (“*King* did not directly address the collection, analysis, and retention of DNA samples from persons who have not been arrested for or convicted of a qualifying offense, leaving open the question of how the Fourth Amendment applies to crime victim, elimination, and suspect samples that have been volunteered to the police.”).

38. Subsequent to the ruling in *Raynor*, the highest court of Massachusetts has also relied upon *King* to reject the claim that DNA analysis of a bloodstained shirt lawfully seized by the police was a search under the Fourth Amendment. See *Commonwealth v. Arzola*, 26 N.E.3d 185, 194 (Mass. 2015) (holding that when “DNA analysis is limited to the creation of a DNA profile from lawfully seized evidence of a crime, and where the profile is used only to identify its unknown source, the DNA analysis is not a search in the constitutional sense”).

privacy in a way that would make his DNA identification unconstitutional.”³⁹ Justice Kennedy explained that the processing of the DNA in *King* identified “noncoding parts of the DNA that do not reveal the genetic traits of the arrestee.”⁴⁰ Indeed, Justice Kennedy dismissed the notion that analyzing biological material to produce a DNA profile reveals any private medical information.⁴¹ Furthermore, even if the testing could reveal private genetic data, Justice Kennedy emphasized that the police “analyze DNA for the sole purpose of generating a unique identifying number against which future samples may be matched.”⁴² Finally, Justice Kennedy pointed to the “statutory protections guarding against further invasion of privacy.”⁴³ There, Justice Kennedy noted that Maryland’s DNA law only permits DNA records related to the identification of persons to be collected, analyzed, and stored, and allows testing for identification purposes only.⁴⁴ In light of these “scientific and statutory safeguards,” the Court concluded that analysis of an arrestee’s DNA “did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment.”⁴⁵

When carefully examined, the last passage—analysis of a DNA sample “did not amount to a *significant* invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment”—is subject to two interpretations.⁴⁶ The passage is vague because Justice Kennedy does not clearly announce that analysis of a DNA sample is not a search. If a challenged police intrusion does not amount to a search, the challenger does not possess an expectation of privacy in the information revealed by the police action. Under the Court’s precedents for determining whether a search has occurred, an expectation of privacy is an all-or-nothing proposition.⁴⁷ Instead of being clear, Justice Kennedy fudges the issue by stating that analysis of a DNA sample “did not amount to a *significant* invasion of privacy.”⁴⁸ However, *Raynor* read *King* to stand for the rule that analysis of a DNA sample does not constitute a search.⁴⁹

At the same time, this passage from *King* can read to stand for the proposition that analysis of a DNA sample, although a search, does not amount to an unreasonable search. Under this reading, analysis of a DNA

39. *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013).

40. *Id.*

41. *Id.* (“The argument that the testing at issue in this case reveals any private medical information at all is open to dispute.”).

42. *Id.*

43. *Id.*

44. *Id.* at 1979–80.

45. *Id.* at 1980.

46. *Id.* (emphasis added).

47. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 744–47 (1979) (holding that a person has no expectation of privacy in the phone numbers dialed from his home).

48. *King*, 133 S. Ct. at 1980 (emphasis added).

49. *Raynor v. State*, 99 A.3d 753, 759 (Md. 2014), *cert. denied*, 135 S. Ct. 1509 (2015).

sample is a reasonable search because it only reveals information related to an arrestee's identification.

Ultimately, *King* does not control the issue resolved in *Raynor* or *Davis*. Indeed, *King* had no reason to address whether a search occurs when the police, without statutory authorization or guidelines, collect and analyze shed DNA samples for investigative purposes. *King* involved the collection and analysis of DNA from a group of persons—those lawfully arrested for serious offenses and held for future prosecution—who possess diminished privacy interests under the Fourth Amendment.⁵⁰ By contrast, persons like Raynor and Davis, not subject to arrest or lawful police detention, enjoy the full protection of the Fourth Amendment vis-à-vis their interactions with the police. For members of the public—“free citizens”—the Fourth Amendment presumes the government will not intrude upon their privacy or possessions, unless there is probable cause or individualized suspicion to do so, or the government has a compelling interest or a “special need” to conduct a suspicionless search or seizure that is unrelated to law enforcement purposes.⁵¹

Moreover, in upholding Maryland's DNA act, *King* stressed that the police exercised no discretion in deciding who was searched.⁵² “The DNA collection is not subject to the judgment of officers whose perspective might be ‘colored by their primary involvement in “the often competitive enterprise of ferreting out crime.”’”⁵³ The same cannot be said about the activities of the police in *Raynor*, *Davis*, and other abandoned DNA cases, in which the police obtain and analyze DNA samples without statutory restrictions or guidelines. “The vast majority of states . . . do not curb or regulate the categories of DNA samples from known persons that may be stored in the

50. See, e.g., *Bell v. Wolfish*, 441 U.S. 520, 557 (1979) (noting privacy expectations of arrestees “necessarily would be of a diminished scope”); *United States v. Chadwick*, 433 U.S. 1, 16 n.10 (1977) (noting that searches of an arrestee are justified in part by the “reduced expectations of privacy caused by the arrest”), *abrogated by California v. Acevedo*, 500 U.S. 565 (1991); cf. *United States v. Robinson*, 414 U.S. 218, 237 (1973) (Powell, J., concurring) (stating that “an individual lawfully subjected to a custodial arrest retains no significant Fourth Amendment interest in the privacy of his person”).

51. See *King*, 133 S. Ct. at 1981 (Scalia, J., dissenting) (“Although there is a ‘closely guarded category of constitutionally permissible suspicionless searches,’ that has never included searches designed to serve ‘the normal need for law enforcement.’ Even the common name for suspicionless searches—‘special needs’ searches—itsself reflects that they must be justified, *always*, by concerns ‘other than crime detection.’” (citations omitted)); see, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995) (applying the special needs doctrine to school officials conducting urine testing of high-school athletes to detect drug use); *Skinner v. Ry. Labor Excs.’ Ass’n*, 489 U.S. 602 (1989) (applying the special needs doctrine to government searches of railroad employees involved in train accidents or safety incidents); *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 668–77 (1989) (applying the special needs doctrine to selected employees of the United States Customs Service subjected to urine tests to detect narcotics use); see also Tracey Maclin, *Is Obtaining an Arrestee’s DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and Will) the Supreme Court Do?*, 33 J.L. MED. & ETHICS 102, 108–15 (2005) (discussing the special needs doctrine and applicability to DNA searches of arrestees).

52. *King*, 133 S. Ct. at 1970 (majority opinion).

53. *Id.* (quoting *Terry v. Ohio*, 392 U.S. 1, 12 (1968)).

state or local databases.”⁵⁴ Put differently, when the police sought Raynor’s DNA, they acted with unfettered discretion.⁵⁵ “This kind of standardless and unconstrained discretion is the evil the Court has discerned when in previous cases it has insisted that the discretion of the official in the field be circumscribed, at least to some extent.”⁵⁶

King is distinguishable from the abandoned DNA cases in another way. When the police obtained King’s DNA sample, he was cognizant of the search.⁵⁷ By contrast, when DNA is secretly obtained and tested, the putative suspect is ignorant of the police intrusion. The covert nature of the police operation appears to exacerbate the intrusion for someone like Raynor, who expressly refused to provide his DNA to the police.⁵⁸

Lastly, *King* does not control cases like *Raynor* or *Davis* because law enforcement officials did not obtain and analyze Raynor’s or Davis’s DNA to identify them; police already knew their identity. “The sole purpose of seizing and searching [their] DNA was to link [Raynor and Davis] to an unsolved crime.”⁵⁹ *King*, on the other hand, rested its holding on the supposed need to identify those arrested for serious offenses.⁶⁰ Indeed, the need to identify arrestees was the critical principle that justified the search in *King*.⁶¹

54. Mercer & Gabel, *supra* note 37, at 655.

55. See also Kreag, *supra* note 24, at 1497 (stating that local DNA databases, operated by local and state police independent of the federal CODIS, run and supervised by the FBI, “increase distributional inequities because local police have total discretion about who to target for inclusion in these databases. This has resulted in police seeking out the ‘usual suspects’—poor people of color—to secure DNA samples for these databases.”); *id.* at 1527 (noting that the inclusion in local databases of DNA profiles “from suspects, not just those arrested or convicted of crimes, gives local law enforcement officials tremendous discretion in building their local databases”); Mercer & Gabel, *supra* note 37 (noting that when police obtain DNA samples from someone not under arrest, the “privacy concerns for these individuals are amplified, because at each stage in the collection and use of volunteered DNA, a police officer must exercise his discretion without guidance from a generally applicable statute uniformly applied to all nonoffenders”); *cf.* Joh, *supra* note 10, at 865 (stating that when police collect and analyze abandoned DNA, “existing Fourth Amendment law appears not to apply at all”).

56. *Delaware v. Prouse*, 440 U.S. 648, 661 (1979).

57. *King*, 133 S. Ct. at 1966.

58. Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Petitioner at 10–11, *Raynor v. Maryland*, 135 S. Ct. 1509 (2015) (No. 14-885), 2015 WL 738571 [hereinafter Brief of Amicus Curiae Electronic Frontier Foundation]. If the Court were to address the issue discussed here, I doubt that it would place much weight on this point. In many of the seminal privacy cases, for example, *Kyllo v. United States* and *Katz v. United States*, the target was unaware of the police intrusion. See *Kyllo v. United States*, 533 U.S. 27, 29–31 (2001); *Katz v. United States*, 389 U.S. 347, 348 (1967). Such unawareness rarely matters when deciding whether a search has occurred. Although the *Katz* test does consider the subjective nature of the target’s privacy interest, ultimately what matters is the objective nature of the privacy interest, i.e., is this an interest society is prepared to accept? See Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 122 (2015) (arguing that the subjective prong of the *Katz* test has been altered; only the objective prong matters).

59. Brief of Amicus Curiae Electronic Frontier Foundation, *supra* note 58, at 11.

60. *King*, 133 S. Ct. at 1970–74.

61. See Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161, 177 (2013) (“The most radical aspect of *King* is its reimagining of the idea of ‘identity’ to include criminal history and other information beyond ‘name and social security

For the reasons listed above, the result and logic of *King* do not control the question of whether police analysis of an involuntarily shed DNA sample constitutes a search under the Fourth Amendment. More interesting, although not acknowledged in *King*, is that the Court itself has already addressed whether government analysis of lawfully obtained biological samples constitutes a search.⁶²

In 1989, *Skinner v. Railway Labor Executives' Ass'n* considered whether toxicological collection and testing of blood, breath, and urine samples—to detect the presence of alcohol or drugs—of railroad employees involved in accidents or safety incidents violated the Fourth Amendment.⁶³ In an opinion upholding the procedures, Justice Kennedy held for the Court that collecting the samples was a search.⁶⁴ More pertinent to the topic discussed here, however, was the Court's conclusion concerning the analysis of blood, breath, and urine samples. Regarding testing of a blood sample, *Skinner* explained that the “ensuing chemical analysis of the sample to obtain physiological data is a *further invasion* of the tested employee's privacy interests.”⁶⁵ With respect to testing urine samples, Justice Kennedy acknowledged that collection and analysis of the samples did not require a bodily intrusion.⁶⁶ Nevertheless, and unlike his opinion in *King*, Justice Kennedy spoke plainly in *Skinner* when he stated that analysis of the samples constituted a search: “It is not disputed, however, that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic.”⁶⁷ To leave no doubt about his conclusion on this matter, Justice Kennedy closed this section of *Skinner* with the following statement: “Because it is clear that the collection and testing of urine intrudes upon expectations of privacy that society has long recognized as reasonable, . . . these intrusions must be deemed searches under the Fourth Amendment.”⁶⁸

Skinner's conclusion that analysis of biological samples constitutes a search has been affirmed by the Court.⁶⁹ Most recently, in *Ferguson v. Charleston*, the Court explained, relying on *Skinner*, that urine tests conducted by state actors to determine whether pregnant women had used illegal drugs during their pregnancies “were indisputably searches within the

number”); Tracey Maclin, *Maryland v. King: Terry v. Ohio Redux*, 2013 SUP. CT. REV. 359, 397 (2014) (“Because the Court's precedents offered no support for Kennedy's position, he had to create an expansive and novel definition of ‘identity’ in order to uphold DNA searches of arrestees.”).

62. See *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 624–33 (1989).

63. *Id.*

64. *Id.* at 616–18.

65. *Id.* at 616 (emphasis added).

66. *Id.* at 617.

67. *Id.*

68. *Id.*

69. See, e.g., *Ferguson v. Charleston*, 532 U.S. 67 (2001).

meaning of the Fourth Amendment.”⁷⁰ In a footnote, *Ferguson* explained that the constitutional status of such tests did not turn on whether test results were reported to law enforcement officials.⁷¹ The soundness of this constitutional rule had not been questioned prior to *King*.

If government analysis of urine samples taken from heavily regulated workers like railroad employees, who have diminished privacy interests “by reason of their participation in an industry that is regulated pervasively to ensure safety,”⁷² amounts to a search under the Fourth Amendment, it is not so obvious why similar analysis by police officials of biological residue left by a free citizen on a discarded straw, a cigarette butt, or an armrest in a police station is not equally a search. As Professor D.H. Kaye wrote in 2001, “all the forms of DNA sampling” should be deemed searches because DNA sampling is close to urinalysis in that subsequent biochemical testing can reveal “private medical facts.”⁷³

Perhaps, when Justice Kennedy wrote in *King* that analysis of an arrestee’s DNA sample “did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment,” he was simply finding that such analysis was not a search under the Fourth Amendment in light of the diminished privacy interests of arrestees held for future prosecution and the state’s legitimate interest in knowing the arrestee’s criminal history.⁷⁴ If that is what Justice Kennedy meant, then *King* does not support concluding that analysis of an abandoned DNA sample collected from a free citizen is also not a search. A contrary conclusion—the conclusion reached in *Raynor*—conflicts with what Justice Kennedy said twenty-four years earlier in *Skinner* when he ruled that analysis of biological samples “must be deemed Fourth Amendment searches.”⁷⁵

III. TENSION BETWEEN CASES

If *King* intended to hold that analysis of human biological samples, whether the sample is saliva, blood, urine, skin, or hair, is not to be considered a search under the Fourth Amendment, then the tension between what Justice Kennedy said in *King* about chemical analysis of biological samples and what

70. *Id.* at 76.

71. *Id.* n.9 (explaining that under its special needs cases, the Court has “routinely treated urine screens taken by state agents as searches within the meaning of the Fourth Amendment even though the results were not reported to the police”).

72. *Skinner*, 489 U.S. at 627.

73. D.H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL’Y 455, 480, 482 (2001) (internal quotation omitted); cf. Kaye & Smith, *supra* note 9, at 444 (“[T]he sensitive nature of some of the information locked in the helices of the DNA molecule leads us to believe that DNA sampling is a Fourth Amendment search, even if the sample is obtained noninvasively.”).

74. *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013).

75. *Skinner*, 489 U.S. at 618.

he said in *Skinner* is obvious.⁷⁶ Of course, one could argue that *King*'s determination that analysis of an arrestee's DNA sample was not a search turned on the fact that the analysis only disclosed "noncoding parts of the DNA that do not reveal the genetic traits of the arrestee."⁷⁷ Moreover, even if the noncoding regions of the DNA, otherwise known as junk DNA, could reveal some genetic information, "[i]t is undisputed that law enforcement officers analyze DNA for the sole purpose of generating a unique identifying number against which future samples may be matched."⁷⁸ In other words, the analysis of the DNA sample in *King* only revealed an arrestee's identification or unique DNA profile.⁷⁹ It was no different than police analysis of a fingerprint,⁸⁰ a voice or handwriting exemplar,⁸¹ or a photograph of someone's face,⁸² all information not protected by the Fourth Amendment.

The problem with this position is that a similar argument could have been utilized in *Skinner* to find that analysis of blood, urine, and breath did not constitute a search. The analysis of blood and urine samples in *Skinner* was done "to detect and measure alcohol and drugs" in the bodies of railroad workers involved in accidents and safety violations.⁸³ There was no evidence that analysis was performed to "reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic."⁸⁴ The same was true for the breath tests in *Skinner*: "breath tests reveal the level of alcohol in the employee's bloodstream and nothing more."⁸⁵ Similar to the blood tests upheld in *Skinner*, "breath tests reveal no other facts in which the employee has a substantial privacy interest."⁸⁶ Thus,

76. See *id.* *King*, 133 S. Ct. at 1979–80.

77. *King*, 133 S. Ct. at 1979.

78. *Id.*

79. David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095, 1142–43 (2013) [hereinafter Kaye, *A Fourth Amendment Theory*] ("For practical purposes, 'the DNA profile derived from the defendant's blood sample establishes only a record of the defendant's identity'—at least, for now. . . ." (footnote omitted)); D.H. Kaye, *Science Fiction and Shed DNA*, 101 NW. U. L. REV. COLLOQUY 62, 62–63 (2006) [hereinafter Kaye, *Science Fiction*] (asserting that "any claim that the DNA profiles currently used for identification constitute 'predictive medical information' is false").

80. See *Cupp v. Murphy*, 412 U.S. 291, 295 (1973). The Court has not definitively ruled on whether obtaining a person's fingerprints constitutes a search, although it has strongly hinted that no search occurs with fingerprinting because it involves "mere 'physical characteristics . . . constantly exposed to the public.'" *Id.* (quoting *United States v. Dionisio*, 410 U.S. 1, 14 (1973)).

81. *Dionisio*, 410 U.S. at 3 (voice exemplar); *United States v. Mara*, 410 U.S. 19, 20 (1973) (handwriting exemplar).

82. *Dionisio*, 410 U.S. at 14. In *United States v. Dionisio*, the Court expressed the view that a person's facial features were not protected by the Fourth Amendment. See *id.* ("Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.")

83. *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 610 (1989).

84. *Id.* at 617.

85. *Id.* at 625.

86. *Id.* at 626.

Skinner could have ruled that the analysis of biological samples in that case did not amount to a search because the tests only revealed whether an employee had alcohol or drugs in his body, information not protected by the Constitution in these circumstances.⁸⁷ The fact that the analysis could have revealed more private medical information about an employee is of no constitutional moment because it was undisputed that the tests were performed only to discover alcohol or drugs. In sum, *Skinner* could have relied upon what the particular intrusion actually revealed, rather than what it might reveal, to find that no search occurred.

Skinner's conclusion that chemical testing of urine and blood constitutes a search for Fourth Amendment purposes shows the Court was concerned with the potential privacy invasion associated with governmental analysis of biological materials. *Skinner*'s stance on this point was not an aberration. Twelve years after *Skinner*, the Court adopted a similar approach in *Kyllo v. United States*.⁸⁸ In a majority opinion written by Justice Scalia, *Kyllo* was concerned with the potential for privacy invasion when it ruled that police use of a thermal imaging device to measure the heat escaping from a private home constituted a search.⁸⁹

Kyllo involved police use of a "relatively crude" thermal imaging machine that measures the amount of heat emanating from a home.⁹⁰ The police suspected that Danny Kyllo was growing marijuana in his home, which typically requires high-intensity lamps.⁹¹ The police used the machine to scan Kyllo's home, and the results disclosed by the machine, along with other information, were included in a search warrant application.⁹² A warrant was issued, and a subsequent search of the home disclosed "an indoor growing operation involving more than 100 plants."⁹³ *Kyllo* held that police utilization of a device that is not in general public use to explore details of the home that would previously have been unknowable without physical intrusion constitutes a search.⁹⁴

Although the police conduct in *Kyllo* was conducted on a public street, measured the amount of heat escaping from a home, and revealed no intimate

87. At the time *Skinner* was decided, a police intrusion, even one directed at a private place, that only reveals whether contraband and nothing else is present, does not amount to a search under the Fourth Amendment. See *United States v. Jacobsen*, 466 U.S. 109, 123–24 (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, 706–07 (1983) (holding that a dog sniff of luggage to detect whether narcotics are inside the luggage is not a search under the Fourth Amendment); see also *Illinois v. Caballes*, 543 U.S. 405, 410 (2005) (relying on *Place* to hold that a dog sniff of a vehicle during a lawful traffic stop is not a search under the Fourth Amendment).

88. *Kyllo v. United States*, 533 U.S. 27 (2001).

89. *Id.* at 40.

90. *Id.* at 36.

91. *Id.* at 29–30.

92. *Id.* at 30.

93. *Id.*

94. *Id.* at 40.

details within the home, such as “what hour each night the lady of the house takes her daily sauna and bath,” those facts were constitutionally irrelevant in deciding whether a search occurred.⁹⁵ A contrary rule, Justice Scalia explained, “would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.”⁹⁶ Justice Scalia emphasized the importance of adopting a constitutional rule that takes account of “more sophisticated systems that are already in use or in development.”⁹⁷

As in *Skinner*, when the Court worried about what private medical facts could be revealed by toxicological analysis of blood and urine, when deciding whether a search occurred in *Kyllo*, Justice Scalia was mindful that advancing technology and science threatened “to shrink the realm of guaranteed privacy” protected by the Fourth Amendment.⁹⁸ Put another way, *Skinner* and *Kyllo* were concerned with both the actual and potential disclosure of information revealed by the challenged government conduct. That is why Professor Albert Scherr has asserted that the “*potential* for intrusion on information created an expectation of privacy in *Kyllo* and in *Skinner*.”⁹⁹

Finally, although *California v. Riley* addressed the constitutionality of an undisputed search, the result and reasoning of *Riley* rested in large part on the Court’s concern for potential invasions of privacy, rather than the specific information disclosed by the challenged search.¹⁰⁰ *Riley* and its companion case, *United States v. Wurie*, addressed whether police officers without a warrant may search digital information on a cell phone seized from an individual incident to arrest. After *Riley* was arrested for driving with a suspended license, police conducted two searches of the cell phone found in his pants.¹⁰¹ The searches disclosed a video of young men fighting while someone yelled language related to the “Bloods” street gang, and photographs of *Riley* standing next to a car that police suspected had been

95. *Id.* at 38.

96. *Id.* at 35–36.

97. *Id.* at 36 (footnote omitted).

98. *Id.* at 34; *see also*, Kerr, *supra* note 12, at 802 (explaining that *Kyllo* recognized that its “rule was not needed to resolve the case before it,” and that the Court “justified the broad rule” to “protect the public from the threat of other more nefarious government surveillance technologies—including technologies yet to be invented”).

99. Scherr, *supra* note 10, at 472–73; *see also* Raynor v. State, 99 A.3d 753, 774 (Md. 2014), *cert. denied*, 135 S. Ct. 1509 (2015) (Adkins, J., dissenting) (explaining that in *Kyllo* and *Skinner* “the mere *potential* for intrusion on information created an expectation of privacy” (citing Scherr, *supra* note 10, at 471)). Although it is a minor matter, I disagree with Professor Scherr’s characterization of what was protected in *Skinner* and *Kyllo*. Scherr says, “The *potential* for intrusion on information created an expectation of privacy.” Scherr, *supra* note 10, at 472–73. The potential intrusion did not create the protected privacy interest. The information disclosed by the intrusion, medical facts in *Skinner* and activity inside the home in *Kyllo*, was the information protected by the Fourth Amendment. *See Kyllo*, 533 U.S. at 40; *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 633 (1989). The potential for intrusion did not create an expectation of privacy; that expectation already existed prior to the intrusion.

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

101. *Id.* at 2480.

involved in an earlier shooting.¹⁰² At trial, “police officers testified about the photographs and videos found on the phone, and some of the photographs were admitted into evidence.”¹⁰³ Riley was convicted on several criminal charges associated with that shooting. In *Wurie*, the police opened Wurie’s flip phone after arresting him for a drug transaction. They also searched the phone’s call log, which revealed the phone number to Wurie’s apartment. The fruits of these searches were included in a search warrant application, which resulted in a search warrant that, when executed, disclosed incriminating evidence implicating Wurie in narcotics and weapons offenses.¹⁰⁴

Writing for eight Justices, Chief Justice Roberts’s opinion held that a warrantless search of a cell phone incident to arrest violated the Fourth Amendment. After explaining why the traditional state interests justifying searches incident to arrest, officer safety and preserving evidence, were inapposite and could not justify the search, Chief Justice Roberts explained why “[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person.”¹⁰⁵ He noted that “the possible intrusion on privacy” is much greater than the intrusion associated with a physical item found on a person.¹⁰⁶ Even the most basic cell phone “might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.”¹⁰⁷ Further, the Chief Justice noted: “An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMd.”¹⁰⁸ Additionally, the capacity of cell phones permits the storage “in one place [of] many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.”¹⁰⁹ People who own cell phones, according to Chief Justice Roberts, “keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.”¹¹⁰

Chief Justice Roberts also remarked that “software on a cell phone, or ‘apps,’ offer a range of tools for managing detailed information about all aspects of a person’s life.”¹¹¹ Noting the ubiquity of apps for almost any topic or activity, the Chief Justice remarked that “[t]he average smart phone user

102. *Id.* at 2481.

103. *Id.*

104. *Id.* at 2481–82.

105. *Id.* at 2489.

106. *Id.*

107. *Id.*

108. *Id.* at 2490.

109. *Id.* at 2489.

110. *Id.* at 2490.

111. *Id.*

has installed 33 apps, which together can form a revealing montage of the user's life."¹¹² Further exacerbating the privacy interests related to cell phone searches, Chief Justice Roberts explained that the data "on many modern cell phones may not in fact be stored on the device itself."¹¹³ Some modern cell phones rely on cloud computing "to display data stored on remote servers rather than on the [phone] itself."¹¹⁴ In sum, it is fair to say the *Riley* Court envisioned the threat posed by warrantless police searches of cell phones as unique and unabated. That threat required that the police obtain a warrant before undertaking a cell phone search. "With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"¹¹⁵

Interestingly, the challenged searches in *Riley* and *Wurie* did not come close to the concerns raised by the Chief Justice. None of the searches involved surveillance of Riley's or Wurie's "Internet browsing history," or "a revealing montage of [Riley's or Wurie's] life."¹¹⁶ Nevertheless, the searches were deemed unconstitutional because the Court focused on the "possible intrusion on privacy" that a cell phone search would entail.¹¹⁷ Put simply, *Riley* "pointed out potential intrusions that could result from a data search with no indication they were involved in the particular case before the court."¹¹⁸

The conflict between *King*, on the one hand, and *Skinner*, *Kyllo*, and *Riley*, on the other hand, is obvious. *Riley* imposed new restraints on police authority to search for digital information because of the possible intrusion on privacy.¹¹⁹ In contrast,

The *King* Court avoided any acknowledgement of the personal nature of DNA information, limited its consideration of privacy interests to the specific search involved, overlooked scientific developments in DNA analysis expanding its investigative use to persons who are neither offenders nor even arrestees, disregarded potential scientific developments increasing the information extracted from DNA, and then broadly extended its decision to DNA laws even more intrusive than the one before the court.¹²⁰

Indeed, the Court's differing attitude about Americans' privacy interests exhibited in *King* and *Riley* is quite startling. When compared to what the Court approved in *King*, Chief Justice Roberts's fear that the police might

112. *Id.*

113. *Id.* at 2491.

114. *Id.*

115. *Id.* at 2494–95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

116. *Id.* at 2489–90.

117. *Id.* at 2489 (emphasis added).

118. *People v. Buza*, 180 Cal. Rptr. 3d 753, 771 n.8 (Cal. Ct. App. 2014), *superseded by* 342 P.3d 415 (Cal. 2015).

119. *See Riley*, 134 S. Ct. at 2484 (conceding that a "mechanical application of [the Court's prior precedent] might well support the warrantless searches" of cell phones).

120. *Buza*, 180 Cal. Rptr. 3d at 771 n.8.

examine an arrestee's "frequent visits to WebMd" on his cell phone seems trivial and exaggerated when one considers the facts in *Riley*.¹²¹ To be sure, the average American probably would not want the police reading their Facebook app, but given a choice between the police reading their Facebook messages or analyzing their DNA sample, my sense is that most Americans would find that government analysis and storage of their DNA samples would be a greater threat to privacy.

Concededly, *King* is not the first case in which the Court purposefully avoided discussing the threat to privacy posed by technological and scientific change.¹²² But the tension between what Justice Kennedy said in *King* and what he said in *Skinner* is apparent.¹²³ Unfortunately, the Court has not provided a neutral principle for deciding when the potential for intrusion into personal information matters in Fourth Amendment cases, especially when new technology is involved.

The potential for invading medical and personal privacy should matter when considering the constitutionality of analyzing involuntarily shed DNA. Unlike the process of collecting and testing DNA obtained from those convicted of crime or persons arrested for serious felonies, currently there are no statutory safeguards regulating the actions of police and other governmental officials who obtain, test, and store shed DNA samples.¹²⁴ If analysis of the sample is not considered a search, law enforcement officials can analyze the sample for a host of genetic or personal information without constitutional restraint.¹²⁵ "To be sure, no evidence currently exists that such

121. *Riley*, 134 S. Ct. at 2490.

122. *See, e.g.*, *Dow Chem. Co. v. United States*, 476 U.S. 227, 238 (1986) (acknowledging that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant[; b]ut the photographs here are not so revealing of intimate details as to raise constitutional concerns"); *United States v. Karo*, 468 U.S. 705, 712 (1984) ("[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment."); *United States v. Knotts*, 460 U.S. 276, 283–84 (1983) (dismissing respondent's claim that permitting the government to use electronic beeper technology to follow persons across state lines would allow twenty-four hour surveillance of any citizen in the country without judicial knowledge or supervision: "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."); *see also* *United States v. Jones*, 132 S. Ct. 945, 954 (2012). *Jones* ruled that a search occurred when the government attached a global positioning system (GPS) tracking device to a vehicle and used that device to monitor the vehicle's movements on the streets for twenty-eight days. The holding in *Jones*, however, did not turn on the amount of data disclosed and retained by the government surveillance, but on the trespass associated with attachment of the GPS device. Thus, *Jones* did not decide whether obtaining extensive location data is a search, let alone an unreasonable search.

123. *See supra* Part II.

124. *See* Kreag, *supra* note 24, at 1544–45 (noting that neither the Fourth Amendment nor federal statutory law regulate law enforcement's use of local databases).

125. Scherr, *supra* note 10, at 474 ("The sample could be analyzed for information far beyond that provided by the more standard 13-loci STR testing, including not only skin pigmentation, bio-geographical origin, gender, and eye color but also a host of medical diseases, medical and behavioral predispositions, and perhaps even sexual orientation.").

analysis is occurring.”¹²⁶ Therefore, it appears that law enforcement officials are limiting their analysis to determine whether samples match DNA evidence found at crime scenes in cold cases, “but this limitation is generated by the police themselves.”¹²⁷

Because there are no checks currently in place to prevent law enforcement officials from analyzing shed DNA samples for genetic information, some scholars are alarmed by the potential for the government to analyze DNA samples for a host of genetic traits.¹²⁸ For example, Professor Elizabeth Joh wrote that DNA samples “may one day be used to identify and segregate those who possess a ‘crime gene.’”¹²⁹ Joh goes on to observe that “finding genetic causes for antisocial behavior is the most widely publicized research of ‘behavioral genetics,’” and the “discovery of a ‘crime gene’ could provide justifications for preventive detentions or other means of social control for those identified as genetically predisposed to criminality.”¹³⁰ While some contend that this fear is overblown and unjustified,¹³¹ it is not so obvious why concerns about more expansive use and testing of DNA samples should be easily dismissed.

When the federal CODIS program was initially proposed, privacy advocates worried that the government’s collection and processing of

126. *Id.*

127. Joh, *supra* note 10, at 875. Writing over a decade ago, Professor Joh observed:

Little oversight exists regarding the intentional or accidental inclusion of [abandoned] DNA evidence into CODIS, regardless of whether a positive match is made between the collected sample and existing forensic evidence. Nor do state laws appear to address explicitly how police ought to treat [abandoned] tissue samples and DNA profiles in relation to *state* databanks.

Id. at 875–76 (footnotes omitted).

128. *See, e.g., id.* at 875–77.

129. *Id.* at 876.

130. *Id.* at 876–77 (footnote omitted); *see also* Tania Simoncelli & Barry Steinhardt, *California’s Proposition 69: A Dangerous Precedent for Criminal DNA Databases*, 33 J.L. MED. & ETHICS 279, 284 (2005) (“While law enforcement authorities would like us to believe that the samples will never be used for anything besides catching criminals, an unlimited span of improper uses remain plausible so long as those samples are retained.”); Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309, 368–70 (2010) (urging caution regarding the government’s possession of DNA samples, which poses a substantial threat to privacy). In a more recent article, Professor Joh acknowledges that *King* “hinted at a willingness to reassess the balance of privacy and government utility” in the future “should the government one day be interested in gleaning information from DNA samples other than matching profiles to crime scene samples.” Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 65 (2014).

131. Kaye, *Science Fiction*, *supra* note 79 (dismissing Joh’s concerns as “science-fiction”); *see also* Kaye, *A Fourth Amendment Theory*, *supra* note 79, at 1143–53 (noting that “the limited information that CODIS loci now supply does not begin to approach” the concerns mentioned in *Skinner* about the disclosure of private medical facts); *id.* at 1158 (concluding that if police have slight “motivation to [scrutinize] an arrestee’s health-related and ancestry-informative loci,” if the means to conduct such a search are not readily available, and if the mechanisms for detecting and punishing this type of illegal search “are effective, then the retention of samples should not defeat [a] biometric exception for DNA databanks”); Edward J. Imwinkelried & D.H. Kaye, *DNA Typing: Emerging or Neglected Issues*, 76 WASH. L. REV. 413, 440 (2001) (stating that police have “little incentive to probe areas of the genome that would determine characteristics not discernible to individuals acquainted with a suspect”).

biological materials would not be confined to persons convicted of violent crimes.¹³² We now know those fears were warranted. “CODIS expanded from an initial focus on collecting profiles from offenders convicted of certain violent crimes, to all felony offenders, and now to arrestees.”¹³³ And after originally barring familial searches of DNA samples, “CODIS now permits them in certain circumstances.”¹³⁴ Indeed, in *King* the Justices were informed of, but expressed no concern about, the way federal and state DNA databases have expanded their reach over the years.¹³⁵ Today, the United States has the world’s largest DNA database.¹³⁶ As science and technology advance, it is naïve to think that scientists and government officials will ignore the opportunity to learn about the genetic traits of persons, especially persons convicted or charged with violent crimes.¹³⁷

132. See Kreag, *supra* note 24, at 1533 (stating that privacy advocates feared that once the federal government’s “DNA database was created, it would be too tempting for law enforcement to be able to limit its use, causing the tool to evolve and reach deeper into our lives”).

133. *Id.* (citing Joh, *supra* note 130, at 51).

134. *Id.* As Professor Erin Murphy explains in her outstanding article on familial searching, in the typical DNA database search, police seek the source of biological material left at a crime scene by searching database profiles that exactly match the DNA profile obtained from the crime scene sample. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 292 (2010). By contrast, familial searching looks for partial matches of the crime scene DNA profile to find potential relatives of the source who left the crime scene sample. *Id.* at 297–98. As Murphy describes: “Familial searching refers generally to the idea of looking in a DNA database not for the person who left the crime scene sample, but rather for a relative of that individual.” *Id.* at 297; see also Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 876–77 (2015) (explaining that under familial searching, “individuals who have never been arrested—and whose DNA could not lawfully be placed in a forensic DNA database directly—may nonetheless be identified, surveilled, and arrested based on a partial DNA match to a close relative”).

135. See Elizabeth E. Joh, *Should Arrestee DNA Databases Extend to Misdemeanors?*, in 8 RECENT ADVANCES IN DNA AND GENE SEQUENCES, no. 2, 2014, at 59, 61 (explaining that though *King*’s holding would seem to be confined to compulsory DNA collection to those arrested for “serious” felonies, the Court knew of the federal law permitting collection from *all* arrestees, suggesting that “an offense severity limitation is not essential to *King*’s core rationale”).

136. Solomon Moore, *F.B.I. and States Vastly Expand DNA Databases*, N.Y. TIMES (Apr. 18, 2009), http://www.nytimes.com/2009/04/19/us/19DNA.html?_r=0; see also Joh, *supra* note 130, at 50 (“The United States has used [DNA samples collected from offenders and arrestees] to amass the largest DNA database in the world.”).

137. See, e.g., David Lazer & Viktor Mayer-Schönberger, *Statutory Frameworks for Regulating Information Flows: Drawing Lessons for the DNA Data Banks from Other Government Data Systems*, 34 J.L. MED. & ETHICS 366, 372 (2006) (remarking that the government’s retention of DNA samples “invites re-purposing at a later stage” (emphasis added)); Joh, *supra* note 10, at 877 (“[M]ore expansive DNA analysis would justifiably serve crime control purposes if science identifies markers for criminogenic behaviors, such as high levels of aggression, or for mental illness. For any of these diagnoses, only a single DNA sample would be required.” (footnotes omitted)); see also Kelly Lowenberg, *Applying the Fourth Amendment When DNA Collected for One Purpose Is Tested for Another*, 79 U. CIN. L. REV. 1289, 1304 (2011) (explaining that Alabama and Michigan permit stored DNA samples to be “accessed and tested for medical research”). As interpreted today, Fourth Amendment principles do not restrain the government from conducting such additional searches. See Joh, *supra* note 130, at 63 (“The Fourth Amendment is primarily interested in the legitimacy of *how* information is acquired. If the acquisition is permissible, how the police use that information thereafter is generally not subject to an additional Fourth Amendment challenge.” (footnote omitted)); Erin Murphy, *Back to the Future: The Curious Case of United States v. Jones*, 10 OHIO ST. J. CRIM. L. 325, 330–31 (2012) (“Current Fourth Amendment law

Finally, and most importantly, government officials retain the biological materials that produce the DNA profiles.¹³⁸ This is the most dangerous threat posed by DNA databases to privacy interests under the Fourth Amendment.¹³⁹ Even Professor David Kaye, a proponent of universal DNA testing, concedes: “There is no doubt that the physical samples (as distinguished from the records in the databases) contain a ‘host of private medical facts.’”¹⁴⁰ Justice Kennedy’s opinion in *King* paid scant attention to this concern. Although *King* stressed that Maryland’s DNA law only permitted collection and testing for identification purposes, the Court did not condition its approval of the statute on this statutory safeguard.¹⁴¹ Thus, testing of stored DNA samples for additional genetic information can be authorized by a legislature at any time.¹⁴²

IV. IMPLICATIONS OF LEAVING THE ANALYSIS OF ABANDONED DNA UNREGULATED BY THE FOURTH AMENDMENT

Over forty years ago, Anthony Amsterdam characterized the task confronting the Court when asked to determine whether a challenged governmental intrusion triggers Fourth Amendment protection.¹⁴³ According to Professor Amsterdam, deciding whether police action constitutes a search ultimately requires a “value judgment.”¹⁴⁴ He explained: “It is whether, if the particular form of surveillance practiced by the police is permitted to go

emphasizes acquisition: how did the police acquire the DNA sample or financial record or biometric image? It cares little for what happens next—to what use that information is put.”)

138. See, e.g., *State v. Medina*, 102 A.3d 661, 664 (Vt. 2014) (noting that Vermont statutes allow for the creation of a DNA database for storing DNA samples).

139. See, e.g., *id.* at 682 (“It is also important to note that the DNA samples being seized provide a massive amount of unique, private information about a person that goes beyond identification of that person.”); SHELDON KRIMSKY & TANIA SIMONCELLI, GENETIC JUSTICE: DNA DATA BANKS, CRIMINAL INVESTIGATIONS, AND CIVIL LIBERTIES 235–36 (2011) (“DNA samples, which are stored indefinitely by forensic laboratories . . . have the potential to reveal almost unlimited information about [individuals].”).

140. Kaye, *A Fourth Amendment Theory*, *supra* note 79, at 1155; D.H. Kaye, *Please, Let’s Bury the Junk: The CODIS Loci and the Revelation of Private Information*, 102 NW. U. L. REV. COLLOQUY 70, 81 (2007), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1080&context=nulr_online (acknowledging the “scientifically tenable claim that the DNA *molecules* in a sample are a threat to privacy; [i]t is time to move on from the debate over ‘junk DNA’ and to address realistically the true privacy problems posed by the growing repositories of DNA samples”); Kaye, *Science Fiction*, *supra* note 79, at 65 (“DNA sampling is potentially more threatening than lifting fingerprints. Both traces carry genetic information, but DNA samples usually contain far more of it.”). Professor Kaye contends that “comprehensive and indefinite sample retention is not essential to DNA databases.” Kaye, *A Fourth Amendment Theory*, *supra* note 79, at 1158.

141. *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (“The Court need not speculate about the risks posed ‘by a system that did not contain comparable security provisions.’”).

142. *Cf. Medina*, 102 A.3d at 682 (“While current law limits use of the sample, that law can be amended to allow greater use; the retention of the DNA sample suggests that expanded use is possible in the future.”).

143. See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

144. *Id.*

unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.”¹⁴⁵

The immediate impact of a ruling that analyzing abandoned DNA does not constitute a search would leave law enforcement officials free to collect, analyze, and store anyone’s DNA sample, provided there was no government coercion or trespass involved with obtaining the sample. This would leave police and state officials free to engage in covert efforts to obtain DNA samples. Thus, a city, county, or state could initiate procedures to secretly obtain DNA samples from persons applying for or renewing a driver’s license, from persons registering to vote or actually voting at a polling station, or even from rummaging through peoples’ garbage left out for collection. These efforts to surreptitiously obtain abandoned DNA, and many others, would not violate the Fourth Amendment rights of individuals who have neither committed an offense nor given law enforcement officials reason to suspect that they had committed an offense.

I think many Americans would find such scenarios to be invasions of their privacy, and for good reason. The central purpose of the Fourth Amendment is to protect us from arbitrary searches and seizures by governmental actors. Put another way, unchecked or discretionary police authority is the chief evil the Fourth Amendment was meant to combat. Proponents of universal DNA collection and analysis, however, will say that this scenario is no cause for alarm because the government will only use abandoned DNA for identification purposes. Furthermore, a majority of the Court views DNA identification as “superior” to fingerprinting.¹⁴⁶

145. *Id.* As a practical matter, the “value judgment” described by Professor Amsterdam comes down to whether five or more Justices are comfortable with having the challenged police conduct applied to themselves. During oral arguments for *United States v. Jones*, which considered whether covertly placing a GPS device on a vehicle constituted a search, Chief Justice Roberts posed the following question to Deputy Solicitor General Michael Dreeben: “You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you’re entitled to do that under your theory?” Transcript of Oral Argument at 9, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5360051. Ultimately, Dreeben conceded that under the Government’s argument, federal agents could place GPS devices on the vehicles of all the Justices. *Id.* at 9–10; *see also* *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (noting that “the only thing the past three decades have established about the *Katz* test (which has come to mean the test enunciated by Justice Harlan’s separate concurrence in *Katz*) is that, unsurprisingly, those ‘actual (subjective) expectation[s] of privacy’ that society is prepared to recognize as “reasonable” bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable” (citations omitted)).

146. *King*, 133 S. Ct. at 1976. There is an energetic debate among legal scholars and scientists regarding how much genetic information can be derived from noncoding parts of DNA, so-called junk DNA. Regarding this debate, *King* asserted: “The argument that the testing at issue in this case reveals any private medical information at all is open to dispute.” *Id.* at 1979. This claim was made without citation or explanation. Other courts have been more cautious regarding the claim that junk DNA does not provide medical information. *See, e.g.,* *People v. Buza*, 180 Cal. Rptr. 3d 753, 772 n.9 (Cal. Ct. App. 2014), *superseded by* 342 P.3d 415 (Cal. 2015) (“Questions about how much information may be derived from junk DNA now and in the future have been the subject of much debate in scientific and legal communities, and studies have begun to suggest links between the CODIS loci and susceptibility to certain

I do not know how most Americans would react if it came to light that federal or state officials were engaged in surreptitious efforts to obtain everyone's fingerprints, even if such actions were only designed for identification purposes. We do know, however, the reaction of Americans when it was revealed that the federal government was secretly tracking and storing the phone numbers dialed and received by everyone.¹⁴⁷ Most had a negative reaction and believed that the government invaded everyone's privacy.¹⁴⁸

Although the comparison is not perfect, there are similarities between the collection and analysis of involuntarily shed DNA and the federal government's telephone surveillance program. To understand some of the similarities, we need to go back to *Smith v. Maryland*, in which the Court concluded that police installation of a pen register, which records the telephone numbers dialed from a person's home or office, at a telephone company did not constitute a search.¹⁴⁹ Writing for the majority, Justice Blackmun ruled that a telephone user has no reasonable expectation of privacy in the telephone numbers dialed because they are voluntarily revealed to the phone company and because it is common for phone companies to keep this information in their business records.¹⁵⁰ According to Justice Blackmun, "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."¹⁵¹

diseases, as well as family relationships and ancestry."). Sheldon Krinsky and Tania Simoncelli discuss the possibility that junk loci may be found to correlate with sensitive information even if the junk codi themselves do not contain sensitive coding information. KRIMSKY & SIMONCELLI, *supra* note 139, at 236. For a sampling of the debate, compare Simon A. Cole, *Is the "Junk" DNA Designation Bunk?*, 102 NW. U. L. REV. COLLOQUY 54 (2007), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1082&context=nulr_online; with Kaye, *supra* note 140 and David Kaye, *What the Supreme Court Hasn't Told You About DNA Databases*, PROMEGA (2013), <http://www.promega.com/resources/profiles-in-dna/2013/what-the-supreme-court-hasnt-told-you-about-dna-databases/>. There is no dispute, however, that the DNA samples themselves contain an enormous amount of highly personal information and represent a real threat to privacy once government officials possess the samples. See KRIMSKY & SIMONCELLI, *supra* note 139 ("DNA samples, which are stored indefinitely by forensic laboratories . . . have the potential to reveal almost unlimited information about [individuals].").

147. See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 PM), <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; see also U.S. DEP'T OF JUSTICE, ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 1 (2013), <https://info.publicintelligence.net/DoJ-NSABulkCollection.pdf> (summarizing the "Government's legal basis for an intelligence collection program" that collected and stored the metadata of Americans' telephone calls).

148. *Global Opinions of U.S. Surveillance*, PEW RES. CTR., <http://www.pewglobal.org/2014/07/14/nsa-opinion/table/american-citizens/> (last visited Oct. 23, 2015) (stating that 61% of Americans found it unacceptable for the American government to monitor communications from American citizens).

149. *Smith v. Maryland*, 442 U.S. 735, 745 (1979).

150. See *id.* at 742-43.

151. *Id.* at 743.

Smith followed a long line of precedent in which the Court found that individuals have no privacy interest protected by the Fourth Amendment when they reveal information to a third party.¹⁵² Under this legal theory, individuals assume the risk that, by revealing private information to a third party, the government will gain access to that information—even if individuals assume that the information will not be disclosed and that third parties will not betray their confidence.¹⁵³

On June 6, 2013, Americans learned that the federal government had been operating a secret program that tracked and analyzed telephone numbers dialed and received by almost every person within the United States and between the United States and foreign countries.¹⁵⁴ Under the program, the Foreign Intelligence Surveillance Court orders telephone communications companies to provide telephone “metadata” in bulk to the National Security Agency (NSA).¹⁵⁵ According to the government, telephone metadata “includes information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted.”¹⁵⁶ The content of calls is not revealed to the government.¹⁵⁷

The federal government’s telephone surveillance program is just an exponentially expanded version of what *Smith v. Maryland* already permits. After all, “what metadata is has not changed over time.”¹⁵⁸ The information revealed by the pen register in *Smith v. Maryland* is the same information obtained by the NSA telephone metadata surveillance program. To be sure, as Judge Leon emphasized in an opinion finding the program unconstitutional, “the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the Government about people’s lives.”¹⁵⁹ But that characterization does not alter the fact that when extant Fourth Amendment norms are applied to the NSA program, Americans knowingly reveal the numbers they dial to telecommunication companies.

The point here is not the correctness of *Smith v. Maryland*; rather, my point is to consider the similarities between collecting and analyzing shed DNA and the NSA telephone surveillance program. Both intrusions rely on individuals exposing material to third parties or in the public domain in the absence of government coercion or force; both involve collecting and storing vast amounts of personal information; both intrusions are executed by law enforcement officials without the requisite amount of suspicion traditionally

152. *Id.* at 743–44.

153. *United States v. Miller*, 425 U.S. 435, 443 (1976).

154. *See* U.S. DEP’T OF JUSTICE, *supra* note 147.

155. *Id.*

156. *Id.*

157. *Id.*

158. *Klayman v. Obama*, 957 F. Supp. 2d 1, 35 (D.D.C. 2013), *vacated and remanded per curiam*, 800 F.3d 559 (D.C. Cir. 2015).

159. *Id.* at 35–36.

required by Fourth Amendment norms; and finally, both intrusions yield potential evidentiary fruits that facilitate law enforcement interests.

The Obama Administration has argued that the NSA program does not involve searches under the Fourth Amendment in light of *Smith v. Maryland*.¹⁶⁰ Moreover, even if the collection of telephone metadata amounts to searches, the Administration maintains that under the balancing formula adopted in *King*, the program is constitutional.¹⁶¹ The Administration contends that the program involves a minimal intrusion on the privacy of telephone users and does not collect the content of calls, and that the data captured by the program may be accessed only when the government has a reasonable suspicion that a particular phone number is associated with a specific foreign terrorist group.¹⁶² Because, according to the Obama Administration, “only an exceedingly small fraction of the data collected has ever been seen,” the program is reasonable under the Fourth Amendment.¹⁶³ Put differently, the Administration views the NSA telephone metadata program as a monitoring device that merely collects information related to telephone identification data that has already been revealed to third parties.¹⁶⁴ Of course, government collection and analysis of shed DNA samples can be characterized the same way—the government is merely collecting, testing, and storing DNA identification information.

Even when viewed through the legal lens of the Court’s assumption-of-risk doctrine, I doubt most Americans would approve of the government collecting, analyzing, and storing shed DNA samples. I believe that many Americans would find such a program, like the NSA telephone surveillance program, a threat to their personal privacy, and would derive no comfort from the claim that the government seeks DNA samples only for identification purposes. To paraphrase Professor Amsterdam, most Americans would find this type of monitoring, unregulated by constitutional restraints, a threat to the privacy of citizens in a manner “inconsistent with the aims of a free and open society.”¹⁶⁵

V. CONCLUSION

I have previously noted that the result and logic of *King* seem “to be miles away from” the massive data mining associated with the NSA telephone metadata program.¹⁶⁶ Yet, lawyers for the Obama Administration

160. U.S. DEP’T OF JUSTICE, *supra* note 147, at 19–20.

161. *Id.* at 21.

162. *Id.*

163. *Id.* (citing *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013) for the rule that intrusions on privacy interests are limited when DNA analysis is used to provide only identification information).

164. *See id.* at 20.

165. Amsterdam, *supra* note 143, at 405.

166. Maclin, *supra* note 61, at 402 n.225.

view *King* as persuasive legal authority for the program.¹⁶⁷ The constitutionality of the NSA telephone metadata program or some similar future surveillance program will be decided by the judiciary. Time will tell whether the constitutional arguments of the Obama Administration will prevail.¹⁶⁸ Whatever the outcome in those cases, for the reasons described above, I do not believe that *King* supports collection and analysis of shed DNA samples by police officials. Government analysis of shed DNA is a search under the Fourth Amendment. Thus, allowing government officials unfettered discretion to collect, analyze, and store DNA samples is inconsistent with the central meaning of the Fourth Amendment, which is designed to check the discretionary power of the police.

167. U.S. DEP'T OF JUSTICE, *supra* note 147, at 21.

168. See *Klayman v. Obama*, 957 F. Supp. 2d 1, 42–43 (D.D.C. 2013) (finding the program unconstitutional as applied to particular plaintiffs), *vacated and remanded per curiam*, 800 F.3d 559 (D.C. Cir. 2015); see also *ACLU v. Clapper*, 959 F. Supp. 2d 724, 724 (S.D.N.Y. 2013) (upholding constitutionality of the program), *vacated and remanded*, 785 F.3d 787, 821 (2d Cir. 2015) (“[W]e hold that the text of § 215 [the federal statutory provision that purportedly authorized the NSA program] cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program.”); *id.* at 824 (“Because we conclude that the challenged program was not authorized by the statute on which the government bases its claim of legal authority, we need not and do not reach these weighty constitutional issues. The seriousness of the constitutional concerns, however, has some bearing on what we hold today, and on the consequences of that holding.”).