University of Michigan Journal of Law Reform

Volume 55

2022

Another *Katz* Moment?: Privacy, Property, and a DNA Database

Claire Mena
University of Michigan Law School

https://doi.org/10.36646/mjlr.55.3.another

ANOTHER *KATZ* MOMENT?: PRIVACY, PROPERTY, AND A DNA DATABASE

Claire Mena*

ABSTRACT

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1] The understanding of these words seems to shift as new technologies emerge. As law enforcement's arsenal of surveillance techniques has grown to include GPS tracking, cell phones, and cell site location information (CSLI), the Supreme Court has applied Fourth Amendment protections to these modern tools.[2] Law enforcement continues to use one pervasive surveillance technique without limitations: the routine collection of DNA. In 2013, the Supreme Court in Maryland v. King held that law enforcement may routinely collect DNA upon arrest for a serious crime.[3] This Note discusses the routine collection of DNA and how it ought to be situated within evolving Fourth Amendment doctrine. Given the nature of DNA and growing DNA databases, law enforcement use of DNA—like its use of other surveillance technologies—should be limited by the Fourth Amendment. DNA collection may not fit neatly within Fourth Amendment jurisprudence, but neither did cell phones, GPS tracking devices, or CSLI when the Court chose to include them under such protections.

TABLE OF CONTENTS

* J.D., University of Michigan Law School, 2021; MBE, Johns Hopkins University, 2018. Thank you to Professors Rebecca Eisenberg, Nina Mendelson, Barbara McQuade, and Margo Schlanger for the guidance, encouragement, and feedback. Thank you to my Student Scholarship Workshop classmates for the invaluable feedback and discussion. Thank you to Gundolf S. Freyermuth for the editing and polishing. Most importantly, thank you Leon S. Freyermuth for your constant encouragement, discussion, and tireless editing; I am so grateful.

1. U.S. CONST. amend. IV.

2. *See* Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1831 (2017); United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).

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

INTRODUCTION

Fourth Amendment jurisprudence is always entering a new era. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[4] Yet the meaning of these words shifts and stretches as new technologies are integrated into society. With the addition of GPS tracking, cell phones, and cell site location information (CSLI) to law enforcement's arsenal of surveillance techniques, the Su-

4. U.S. CONST. amend. IV.

preme Court in recent years has attempted to adapt Fourth Amendment jurisprudence to the realities of modern technology.[5] Unlike the search of a home or the objects on an arrestee's body, modern surveillance techniques pose new questions that the founders could not have imagined. The Court is routinely forced to decide how to preserve the values embodied within the Fourth Amendment in light of new surveillance technologies.[6]

Law enforcement is much better equipped to investigate and combat crime today than it was when the Constitution was drafted. A modern wiretap makes it possible to listen to a suspect's phone calls from miles away. A GPS tracking device can map and record every place a suspect visits, providing a comprehensive chronicle of her activities. And a cell phone can provide incriminating pictures, text messages, and search histories, while revealing the most intimate images, conversations, and even thoughts of a suspect and her associates. Beyond private technologies like cell phones and GPS tracking, metadata collection programs subject large swaths of the population to invasive, suspicionless surveillance.[7]

The founders did not contemplate such intrusions on privacy. To track the movements of one person, as a GPS tracker could do, would be nearly impossible, requiring constant monitoring by multiple agents.[8] Similarly, prior to the invention of cell phones, law enforcement could never have gained in-depth personal information about an individual during an arrest. The individual would have had to be carrying a trunk full of personal documents with them at the time.[9] And still, that trunk could not have been searched without a warrant.[10] As Justice Alito noted, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."[11]

Over the years, the U.S. Supreme Court has continued to reckon with new technologies' effect on Fourth Amendment jurisprudence. Technology can greatly improve law enforcement's ability to combat crime, but it comes at a cost to individual and societal privacy. In attempting to protect technologies like cell phones, CSLI, and GPS tracking from government intrusion, the Court has created various carve-

5. *See Jones*, 565 U.S. 400; *Riley*, 573 U.S. 373; *Carpenter*, 138 S. Ct. 2206.

6. Hu, *supra* note 2, at 1831 ("[T]he Court has been forced to grapple with how best to preserve the integrity of the Fourth Amendment in light of technological advances."); *see Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring).

7. Hu, *supra* note 2, at 1824.

8. *Jones*, 565 U.S. at 429 (Alito, J., concurring).

9. *Riley*, 573 U.S. at 394.

10. *Id.*

11. *Jones*, 565 U.S. at 429 (Alito, J., concurring).

outs to Fourth Amendment doctrine, leaving the jurisprudence without a "clear, unifying data privacy doctrine."[12]

In contrast to its attempts to protect cell phones, CSLI, and GPS, the Court has made no attempt to protect one major surveillance technology: the routine collection of DNA. DNA, under the express holding in *Maryland v. King*, may be systematically collected by law enforcement upon arrest for a serious crime.[13]

This Note focuses on DNA collection to illustrate ongoing challenges with Fourth Amendment doctrine and its relationship to new technologies. DNA collection presents a particularly interesting conundrum: like the search of a cell phone or the use of a GPS-tracking device, DNA collection is a search of an individual. With the systematic storage of DNA profiles in private and law enforcement databases that can be searched later, however, DNA collection is also similar to mass surveillance.

Interestingly, scholarship regarding DNA collection and the *King* decision are largely separate from scholarship about Fourth Amendment doctrine and its relationship to new surveillance technologies. This Note bridges these two areas, using DNA collection to demonstrate the pitfalls of the ever-evolving Fourth Amendment doctrine.

Part I of this Note provides background on Fourth Amendment doctrine and its relationship to new surveillance techniques. Part II discusses law enforcement's use of DNA and how DNA collection falls outside the protections of the Fourth Amendment. The legality of DNA collection illustrates three issues that arise with Fourth Amendment doctrine: (1) the evolving and advancing nature of surveillance technology; (2) highly fact-specific inquiries, resulting in narrow holdings that often fail to reflect the reality of, or constrain, law enforcement activities; and (3) a focus on individual harms, rather than the collective harm to society, which leaves many without recourse. Part III proposes solutions to address both Fourth Amendment doctrine and DNA collection; while scholars have proposed solutions to both, they are often treated as separate topics in the literature. This Note advocates for incorporating DNA collection within the proposed solutions to Fourth Amendment doctrine.

12. Hu, *supra* note 2, at 1827.
13. Maryland v. King, 569 U.S. 435, 435 (2013).

I. STATE OF THE FOURTH AMENDMENT: AN UNSTABLE DOCTRINE & EVOLVING TECHNOLOGY

Part I discusses the evolution of the Fourth Amendment and recent surveillance cases. According to Professor Margaret Hu, "[i]t is undisputed that the Court has been forced to grapple with how best to preserve the integrity of the Fourth Amendment in light of technological advances."[14] In the context of surveillance techniques, this dilemma produces Fourth Amendment jurisprudence without a clear doctrine; the Court addresses new techniques by creating carve-outs and exceptions in the recent cases discussed below.[15] The evolution of the doctrine, as described in Part I, suggests why DNA collection is unprotected from government intrusion.

A. *The Evolving View of a Wiretap:* Olmstead *&* Katz

Fourth Amendment jurisprudence was originally based on common law trespass—the idea that law enforcement could not enter one's home or touch one's property without a warrant.[16] The trespass test, however, had limitations. In the 1920s, FBI agents wiretapped the phone lines of a suspect's home and office to surveil a bootlegging operation.[17] The U.S. Supreme Court, in its decision in *Olmstead v. United States*, determined that the government did not trespass upon the Mr. Olmstead's property.[18] A wiretap, unlike a traditional search, did not intrude upon "materials things—like the person, the house, his papers, or his effects," as the agents connected the phoneline outside the parameters of Mr. Olmstead's property.[19]

This trespass-based understanding of the Fourth Amendment began to shift after *Olmstead*.[20] In another wiretapping case, the Court in *Katz v. United States* rejected the trespass-based test and held that the Fourth Amendment "protects people, not places."[21] Mr. Katz closed the

---

14. Hu, *supra* note 2, at 1831.

15. *Id*. at 1827.

16. *See Jones*, 565 U.S. 400; Carpenter v. United States, 138 S. Ct. 2206 (2018). Orin Kerr disagrees with the premise. He notes that this is the popular view of scholars, but that the doctrine did not have an articulated property test as described by the Court and scholars. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67 (2013). The Supreme Court, however, has articulated this view, and based decisions upon this view, in cases including *Carpenter* and *Jones*. 565 U.S. 400; 138 S. Ct. 2206.

17. Olmstead v. United States, 277 U.S. 438, 455 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967) *and* Berger v. New York, 388 U.S. 41 (1967).

18. Hu, *supra* note 2, at 1836; *Olmstead*, 277 U.S. at 457.

19. *Olmstead*, 277 U.S. at 464; U.S. CONST. amend. IV.

20. *See* Hu, *supra* note 2, at 1836; *Katz*, 389 U.S. 347.

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

door to the public phone booth in which the wiretapping occurred, demonstrating his "reasonable expectation of privacy."[22] Thus, the landmark "reasonable expectation of privacy" test was born and it remains foundational to Fourth Amendment jurisprudence.[23]

According to the *Katz* Court, reading the Constitution under the original trespass doctrine, as it did in *Olmstead*, would "ignore the vital role that the public telephone has come to play in private communication."[24] *Katz* demonstrates the onset of an important theme in Fourth Amendment surveillance cases: the Court shifted the doctrine to reflect the *spirit* of the Fourth Amendment, essentially protecting society from governmental misuse of a new surveillance technology.

B. *Carve Outs and Exceptions: The Supreme Court Adapts Fourth Amendment Doctrine to Address Emerging Surveillance Technologies*

The *Katz* dilemma persists as new technologies are integrated into society and become a part of law enforcement's surveillance techniques. Fourth Amendment doctrine is often ill-equipped to address complex issues posed by new technologies. In three recent cases discussed below—*United States v. Jones*, *Riley v. California*, and *Carpenter v. United States*—the Court created exceptions or carve-outs to the existing doctrine.

1. GPS Tracking Devices: An Exception to the Reasonable Expectation of Privacy Test

In recent years, the Court has stepped back from the reasonable expectation of privacy test, implicitly acknowledging that *Katz* is not always equipped to address certain surveillance techniques.[25]

The *Katz* test had long been the subject of wide criticism.[26] According to Justice Alito, the *Katz* approach presumes that the "hypothetical reasonable person has a well-developed and stable set of privacy expectations."[27] The technology itself can shift such privacy expectations as it

---

22. *Id.* at 352.

23. Steven I. Friedland, Riley v. California *and the Stickiness Principle*, 14 DUKE L. & TECH. REV. 121, 131 (2016); *see, e.g.*, *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Justice Harlan in his *Katz* concurrence defines the criteria to determine whether a reasonable expectation of privacy exists. This includes (1) whether the "person . . . exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361.

24. *Katz*, 389 U.S. at 352.

25. *See* United States v. Jones, 565 U.S. 400, 403 (2012).

26. Hu, *supra* note 2, at 1829; *Jones*, 565 U.S. at 427.

27. Hu, *supra* note 2, at 1887; *Jones*, 565 U.S. at 427 (Alito, J., concurring).

becomes more integrated into society.[28] As individuals become more reliant on their devices, the technology seems less intrusive.[29] Eventually, it can "diminish societal and individual expectations of privacy."[30] In today's world, only an "out-of-touch Luddite" could escape such surveillance.[31]

The *Katz* dilemma arose again in the context of GPS tracking devices in *United States v. Jones*, where FBI agents attached the device to a suspected drug trafficker's car.[32] The case seemed to fit squarely within already settled law.[33] Generally, individuals do not hold a reasonable expectation of privacy in their movements; Mr. Jones could not expect privacy on the underside of his car nor in his location on public roads.[34] Instead, the Court—shifting from the decades-long focus on privacy—held that the use of the GPS tracking device attached to Mr. Jones's property constituted a trespass, and therefore an unreasonable search under the Fourth Amendment.[35]

Justice Sotomayor's concurrence maintained the *Katz*-based privacy theory, drawing upon a "'mosaic' theory" of the Fourth Amendment.[36] While each individual location spot may not raise serious privacy concerns, Justice Sotomayor found something more invasive about continual GPS monitoring amounting to 2,000 pages of location data.[37] Information collected in the aggregate can reveal sensitive information about a person over time, including intimate details such as political and religious beliefs, or even sexual habits.[38]

The emergence of new technologies strains the "reasonable expectation of privacy" test. Just because a technology shifts society's expectation of privacy does not necessarily mean that an individual's Fourth Amendment protections should diminish. These concerns appear to

---

28. *Jones*, 565 U.S. at 427 (Alito, J., concurring).

29. Hu, *supra* note 2, at 1828–29.

30. *Id.* at 1829.

31. *See Jones*, 565 U.S. at 403.

32. *Id.*

33. Herbert W. Titus & William J. Olson, United States v. Jones*: Reviving the Property Foundation of the Fourth Amendment*, 3 CASE W. RSRV. J.L. TECH. & INTERNET 243, 243 (2012).

34. *Jones*, 565 U.S. at 412 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

35. Titus & Olson, *supra* note 33, at 247; *Jones*, 565 U.S. at 404. According to the Court, there was no need to address Mr. Jones's reasonable expectation of privacy, as his Fourth Amendment rights did not "rise or fall with the *Katz* formulation." 565 U.S. at 406. While recent jurisprudence focused on privacy, the Fourth Amendment continued to protect individuals from the trespass of government.

36. Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 420 (2019); Titus & Olson, *supra* note 33, at 249.

37. Titus & Olson, *supra* note 33, at 249; *see Jones*, 565 U.S. at 403, 413–18 (Sotomayor, J., concurring).

38. Harvey Gee, *Almost Gone: The Vanishing Fourth Amendment's Allowance of Stingray Surveillance in a Post-Carpenter Age*, 28 S. CAL. REV. L. & SOC. JUST. 409, 425 (2019); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

animate the decision in *Jones*. There, as in *Katz*, the Court shifted the doctrine to protect the spirit of the Fourth Amendment.

2. The Cell Phone: An Exception to the Search Incident to Arrest Doctrine

Since *Jones*, the Court has continued to grapple with law enforcement's use of new technologies. In *Riley v. California*, the Court determined that a warrantless search of an arrestee's cell phone is an unreasonable search under the Fourth Amendment.[39] The Court noted that an officer's search of a cell phone raises a host of privacy concerns because cell phones contain internet browsing history, apps, phone records, calendar appointments, and an immense data storage capacity.[40]

Because the search of the cell phone occurred during an arrest, the Court applied the "search incident to arrest" doctrine.[41] A search incident to arrest must be "limited to the area within the arrestee's immediate control" and "justified by the interests in officer safety and in preventing evidence destruction."[42] Applying the doctrine to cell phones, the Court noted that digital data on a cell phone cannot be used as a weapon to harm an officer or assist an arrestee's escape.[43] The Court further noted that the government's concerns regarding preservation of evidence, including remote wiping, can largely be overcome.[44]

Ultimately, given the privacy concerns implicated by searching a cell phone, the Court held that law enforcement may not search a cell phone seized during an arrest without a warrant.[45] Effectively, the Court established an exception to the categorical rule in *United States v. Robinson*, which allows for the search of a suspect's possessions incident to an arrest.[46] Cell phones, unlike other things typically found on an arrestee, cannot be searched by law enforcement.[47] Again, the Court created a carve-out to a well-established doctrine to protect against law enforcement abuse of a new technology.

---

39. Friedland, *supra* note 23, at 135; Riley v. California, 573 U.S. 373, 373 (2014).

40. *Riley*, 573 U.S. at 394.

41. *Id.* at 382–83 (outlining the doctrine as established in Chimel v. California, 395 U.S. 752 (1969); United States v. Robinson, 414 U.S. 218 (1973); Arizona v. Gant, 556 U.S. 332 (2009)).

42. Friedland, *supra* note 23, at 132–33 (describing the search incident to arrest doctrine in the context of *Riley*); *Riley*, 573 U.S. at 374; *see Chimel*, 395 U.S. 752.

43. *Riley*, 573 U.S. at 374.

44. *Id.* at 390.

45. *Id.* at 388; Friedland, *supra* note 23, at 135.

46. *See* Friedland, *supra* note 23, at 135–36; *Riley*, 573 U.S. at 374. In *Robinson*, "the Court applied the *Chimel* analysis to a search of a cigarette pack found on the arrestee's person. It held that the risks identified in *Chimel* are present in all custodial arrests." *Riley*, 573 U.S. at 374 (citation omitted); *Robinson*, 414 U.S. at 235.

47. *Riley*, 573 U.S. at 388; Friedland, *supra* note 23, at 135.

3. CSLI: An Exception to the Third Party Doctrine

Like in *Riley*, in *Carpenter v. United States*, the Court created an exception to settled doctrine to protect CSLI from government intrusion.[48] In *Carpenter*, law enforcement obtained the suspect's CSLI from a telecommunications company, which placed him at the scene of the robberies.[49] Unlike in *Riley*, where the Court applied the "search incident to arrest doctrine," the Court in *Carpenter* applied the "third-party doctrine."[50] The third-party doctrine holds that a person who "voluntarily" conveys data to a third party has no reasonable expectation of privacy in those data.[51] Thus, if law enforcement accesses the data, it is not considered a search under the Fourth Amendment. The third-party data typically at issue includes records created and maintained by phone companies, internet service providers, hotels, and banks.[52]

Breaking with traditional third-party doctrine, the Court held that collecting the suspect's CSLI constituted a search under the Fourth Amendment.[53] When the government accessed the CSLI, it obtained a "comprehensive chronicle of the user's past movements."[54] Drawing upon Justice Sotomayor's concurrence in *Jones*, the Court noted the nature of the information collected.[55] Mapping a person's location over time can reveal private information including "familial, political, professional, religious, and sexual associations."[56] Since people tend to carry their cell phones everywhere, obtaining a person's CSLI is like placing an ankle monitor on them without their knowledge.[57]

Carpenter's holding is narrow: according to the Court, Mr. Carpenter had a protected interest in CSLI revealing his movements for seven days or more.[58] That said, *Carpenter* represents a greater shift in the Court's thinking. The Court "refused to allow the third-party doctrine to

---

48. Gee, *supra* note 38, at 423; *see* Carpenter v. United States, 138 S. Ct. 2206 (2018).

49. *See Carpenter*, 138 S. Ct. at 2212–13.

50. *See id.* at 2216; *Riley*, 573 U.S. at 382; Friedland, *supra* note 23, at 132–33.

51. *Carpenter*, 138 S. Ct. at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)); *see* United States v. Miller, 425 U.S. 435 (1976).

52. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third-Party Doctrine*, 130 HARV. L. REV. 1924, 1931 (2017). That note explained that the district court in *United States v. Suarez-Blanca*, No. 07-CR-0023, 2008 WL 4200156, at *7 (N.D. Ga. Apr. 21, 2008), applied the exception to "(1) bank records; (2) credit card statements; (3) kilowatt consumption from electric utility records; (4) motel registration records; (5) cell phone records; and (6) employment records." *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third-Party Doctrine*, *supra*, at 1931; *see Miller*, 425 U.S. at 444.

53. *Carpenter*, 138 S. Ct. at 2223.

54. *Id.* at 2211.

55. *Id.* at 2215; Gee, *supra* note 38, at 425; *see* United States v. Jones, 565 U.S. 400, 414–16 (2012) (Sotomayor, J., concurring).

56. Caminker, *supra* note 36, at 424; *Carpenter*, 138 S. Ct. at 2217 (citations omitted).

57. *Carpenter*, 138 S. Ct. at 2217–18; *see* Caminker, *supra* note 36, at 424.

58. Caminker, *supra* note 36, at 424.

swallow the Fourth Amendment in the digital age."[59] Once again—like in *Katz*, *Jones*, and *Riley*—the Court adapted Fourth Amendment doctrine to address the impact of a new technology.

C. *The Missing Piece of the Fourth Amendment Test: Collective Harms*

Katz, *Jones*, *Carpenter*, and *Riley* all have one key thing in common: each defendant demonstrated standing based on the individual harm they experienced from government surveillance.[60] Each decision, however, produced a societal benefit that extended beyond that defendant. The Court, as David Doernberg writes, "is operating under different and inconsistent theories of Fourth Amendment rights and remedies."[61] For example, Mr. Jones was individually harmed when law enforcement intruded upon his personal property by using the GPS-tracking device, but the Court's remedy was collective.[62] Because of *Jones*, law enforcement officers must obtain a warrant prior to using a GPS-tracking device.

This focus on collective harms may not stray far from the original meaning of the Fourth Amendment. The Fourth Amendment may serve two purposes: (1) to protect the right of the individual, and (2) "to prevent the government from functioning as in a police state."[63] Fourth Amendment jurisprudence has largely focused on the first purpose.[64] However, many scholars argue that the text of the Fourth Amendment guarantees the right to people as a group.[65] The "right to be secure," not only protects individuals from being searched unreasonably, but provides for a societal right to be free from the anxiety generated by such intrusive practices.[66]

---

59. Natalie Ram, *Genetic Privacy After Carpenter*, 105 VA. L. REV. 1357, 1374 (2019); *see also* Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 358–59 (2019).

60. *See* Katz v. United States, 389 U.S. 347 (1967); *Carpenter*, 138 S. Ct. 2206; *Jones*, 565 U.S. 400; Riley v. California, 573 U.S. 373 (2014).

61. Donald L. Doernberg, *The Right of the People: Reconciling Collective and Individual Interests Under the Fourth Amendment*, 58 N.Y.U. L. REV. 259, 283 (1983) ("This inconsistency has been explored at some length . . . [previously by John M.] Burkoff"); *see also* John M. Burkoff, *The Court That Devoured the Fourth Amendment: The Triumph of an Inconsistent Exclusionary Doctrine*, 59 OR. L. REV. 151 (1979).

62. Doernberg, *supra* note 61, at 283.

63. *Id.* at 260.

64. *See Id.*

65. *See, e.g.*, *id.* at 260–61; David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH L. REV. 189, 199 (2015).

66. Richard H. McAdams, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 318–19 (1985).

Under Fourth Amendment doctrine, it is difficult to address the collective harms absent an individual harm.[67] In *Clapper v. Amnesty International*, a group of attorneys, journalists, and activists challenged the constitutionality of a surveillance program under Section 702 of the Foreign Surveillance Intelligence Act (FISA).[68] The outcome of *Clapper* hinged on whether the plaintiffs had standing.[69] The Court held that the plaintiffs failed to show an impending future injury and that the future injury would be "fairly traceable" to the specific FISA provision.[70] As a result, the government's FISA program was essentially shielded from Fourth Amendment review.[71] The case demonstrates that where there is a collective harm, rather than an individual harm, plaintiffs may be precluded from challenging certain surveillance programs because they lack standing.[72]

In light of modern surveillance programs, the collective approach is appealing. When Edward Snowden disclosed the National Security Agency's bulk collection programs, many Americans were outraged at the government's widespread collection of phone and internet metadata.[73] Although most individuals were not directly harmed, or at least made aware of how they may have been harmed, many felt the government had intruded into their private lives.[74] Ultimately, given the nature of emerging surveillance technology, it may be useful to view certain invasions as collective intrusions of privacy, rather than individual intrusions.[75]

II. DNA LEFT UNPROTECTED BY THE DOCTRINE

Against this backdrop of Fourth Amendment jurisprudence, Part II discusses law enforcement use of DNA and the *Maryland v. King* decision, in which the U.S. Supreme Court expressly sanctioned law enforcement collection of DNA. Part II concludes by focusing on three issues inherent to Fourth Amendment doctrine as applied to DNA: (1)

---

67. *See* David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 92 (2018); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 400 (2013).

68. *Clapper*, 568 U.S. at 398.

69. *See id.* at 390–400.

70. *Id.*

71. Gray, *supra* note 67, at 92.

72. *See id.*

73. *See* A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RSCH. CTR. (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ [https://perma.cc/QD5J-H9LF]; Margaret Hu, *Taxonomy of the Snowden Disclosures*, 72 WASH. & LEE L. REV. 1679 (2016).

74. *See* Geiger, *supra* note 73

75. Doernberg, *supra* note 61, at 260.

the evolving and advancing nature of surveillance technology; (2) highly fact-specific inquiries, which result in narrow holdings that often fail to reflect the reality of, or constrain, law enforcement activities; and (3) a focus on individual harms, rather than the collective harm to society, which leaves many without recourse.

A. *DNA Under the Fourth Amendment:* Maryland v. King

In *Maryland v. King*, Mr. King was arrested for first- and second-degree assault.[76] Upon his arrest, law enforcement collected his DNA.[77] The DNA sample was analyzed and the test results were uploaded to the Maryland DNA database with identifying information.[78] Months later, the test results were matched to a sample taken from an unsolved rape case maintained on the Combined Index Data Systems (CODIS), the federal DNA database.[79] Mr. King challenged the Maryland DNA Collection Act, which allowed law enforcement to use a buccal swab to take a DNA sample upon arrest for a serious offense.[80] The Supreme Court analogized DNA collection to routine fingerprinting that takes place during the booking process for an arrest.[81] As discussed throughout Part II, DNA collection poses additional privacy concerns beyond those of fingerprinting. DNA is laden with intimate details revealing one's genetic history and predispositions. Furthermore, unlike a fingerprint, DNA not only provides information about the individual who is accused of the crime, but also about their family members.[82] Despite these privacy interests, the Supreme Court ultimately found that collecting an arrestee's DNA in connection with a serious offense is not an unreasonable search under the Fourth Amendment.[83]

---

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

77. *Id.* at 441.

78. *Id.* at 472 (Scalia, J., dissenting).

79. *Id.* at 441, 444–45; Craig M. Bradley, *Cheek Swabs, DNA, and Delay*, 2013 SUP. CT. REV. 54.

80. *King*, 569 U.S. at 441.

81. *Id.* at 436.

82. *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet#:~:text=What%20is%20CODIS%3F%20CODIS%20is%20the%20acronym%20for,as%20the%20software%20used%20to%20run%20these%20databases [https://perma.cc/X77L-FHP3] (noting that familial searches are not performed on the federal level but are performed on the state level including in Arkansas, California, Colorado, Florida, Michigan, Texas, Utah, Virginia, Wisconsin, and Wyoming).

83. David H. Kaye, *Why So Contrived? Fourth Amendment Balancing, Per Se Rules, and DNA Databases After* Maryland v. King, 104 J. CRIM. L. & CRIMINOLOGY 535, 535 (2014); *see King*, 569 U.S. at 435.

1. The Supreme Court's Understanding of DNA Fails to Capture the Privacy Interests at Stake

The Court largely based its reasoning on a distinction between coding DNA and non-coding DNA.[84] Law enforcement traditionally creates DNA profiles using thirteen (now updated to twenty) STR[85] loci from non-coding regions of the genome.[86] Information from the coding regions has been thought to include "more far-reaching and complex characteristics like genetic traits."[87] In contrast, information from the non-coding regions was not believed to pose the same privacy concerns.[88] For example, information regarding one's ethnic makeup or likelihood of developing breast cancer was thought to be outside the bounds of the non-coding region.[89] Essentially, law enforcement selected those loci for their location outside the coding regions, as they were believed to pose few privacy concerns.[90]

The Court drew upon this distinction, noting that the selected loci from the noncoding regions do not contain medical information or reveal sensitive information regarding genetic traits or genetic disease.[91] The Court specifically maintained the notion that the noncoding regions amount to nothing more than "junk DNA."[92] While scientists have largely moved away from this nickname, remnants of this viewpoint animate the Court's analysis in *King*.[93]

The Supreme Court's interpretation of the science contradicted widespread scientific understanding of non-coding regions at the time.[94] In fact, the non-coding regions contain about four million "gene switches" that act as on and off switches for genes.[95] For example, a gene switch in non-coding DNA could instruct a cell in the pancreas to

---

84. *See King*, 569 U.S. at 442–43, 445.

85. Essentially, law enforcement mainly analyzes the DNA by using short tandem repeats (STRs)—short sequences of DNA that differ between individuals. The specific loci were selected because they are located in the non-coding regions of the genome, e.g., the loci are not in the estimated three percent of the genome that consists of genes encoding specific proteins.

86. *See King*, 569 U.S. at 445.

87. *Id.*. at 443.

88. *See Id*.

89. *See generally* Stephen S. Hall, *Hidden Treasures in Junk DNA*, SCI. AM. (Oct. 1, 2012), https://www.scientificamerican.com/article/hidden-treasures-in-junk-dna/ [https://perma.cc/L7SR-WJTA].

90. *See King*, 569 U.S. at 445.

91. *King*, 569 U.S. at 442–43, 445; George M. Dery III, *Opening One's Mouth "for Royal Inspection": The Supreme Court Allows Collection of DNA from Felony Arrestees in* Maryland v. King, 2 VA. J. CRIM. L. 116, 137 (2014).

92. *King*, 569 U.S. at 442, 445.

93. *See id.* at 442–43, 445.

94. Dery, *supra* note 91, at 147.

95. Live Science Staff, *What Is ENCODE, and Why Does It Matter?*, LIVE SCI. (Sept. 6, 2012), https://www.livescience.com/22990-encode-explanation-facts.html [https://perma.cc/3EZZ-A6VP].

create insulin after eating.[96] This major area of the genome actually plays a central role in gene-controlling activity, contributing to hundreds of common medical conditions.[97] As George Derry puts it, "[w]riting off all 'noncoding' DNA as not revealing genetic traits simply flies in the face of evidence provided by some of the world's most prestigious scientific journals."[98] At the very least, there appeared to be more function in these regions of the genome than the Court acknowledged.[99]

Even if the DNA did provide sensitive medical information, the Court reasoned, it was not tested for that purpose.[100] The Court analogized the use of DNA to a drug test.[101] While a drug test can reveal other information—including pregnancy, diabetes, or epilepsy—the blood is tested for one single purpose: drug use.[102] Similarly, while analysis of DNA can be used for a range of reasons, law enforcement had one singular purpose: identification.[103]

The Court further reasoned that, even if such privacy concerns were present, the Maryland Act provided statutory protections to guard against privacy intrusions.[104] The Act ensured that only DNA records directly relating to the identification of the arrestee were stored.[105] Ultimately, the Court reasoned, "the processing of [Mr. King's] DNA sample's CODIS loci did not intrude on his privacy in a way that would make his DNA identification unconstitutional."[106]

2. The Supreme Court Deems DNA Useful for Identification Rather than Investigation to Sidestep the Incident to Arrest Doctrine

In upholding the Maryland DNA Collection Act, the Court reasoned that the government's interest in identifying the arrestee with the DNA outweighed the limited privacy concerns of the arrestee.[107] The claimed government interest—*identification*—perplexed many, including the

96. *Id.*
97. *Id.*
98. Dery, *supra* note 91, at 148.
99. *What Is ENCODE, and Why Does It Matter?*, *supra* note 95; Eliza Strickland, *Enjoy Your Opposable Thumb? Thank Your "Junk" DNA*, DISCOVER (Sept. 5, 2008, 2:35 PM), https://www.discovermagazine.com/planet-earth/enjoy-your-opposable-thumb-thank-your-junk-dna#.XUskjJNKjm [https://perma.cc/Y4Z4-7G4W].
100. Maryland v. King, 569 U.S. 435, 438 (2013).
101. *Id.* at 464.
102. *Id.*
103. *Id.*
104. *Id.* at 465.
105. *Id.*
106. *Id.* at 437; *see also* Dery, *supra* note 91, at 136–38.
107. *See* Kaye, *supra* note 83, at 535; Ram, *supra* note 59, at 1386; *King*, 569 U.S. at 466.

dissent.[108] The government's interest, on its face, appears to be investigating crime.[109] Mr. King's profile was not compared against a database of known offenders, but against the database of profiles from unsolved crimes.[110] Certainly, an unsolved crime could not have identified Mr. King as the perpetrator.

The Court took an expansive view of the meaning of "identity," reasoning that connecting Mr. King to an unsolved crime could inform bail decisions.[111] In theory, a person who has committed previous undetected crimes may be more inclined to flee if he fears his contact with the criminal justice system could expose other crimes.[112] Such a connection could also provide information as to whether he may have a violent history and be a risk to the victim, the public, or even detainees and facility staff as he awaits bail.[113]

Even if the government's interest was identification, rather than crime-solving, the use of DNA under the Maryland Act did not appear to effectuate this interest. Mr. King's DNA was not analyzed, and his profile was not uploaded, until months after his arrest.[114] The Maryland Act specifically prohibits the analysis and uploading of DNA prior to the first arraignment.[115] Surely, as Justice Scalia pointed out in his dissent, the lower court did not arraign Mr. King without knowledge of his identity.[116]

So, why did the Court focus on identity? If the Court recognized the government's interest as "investigation of crime," it may have had no choice under existing doctrine but to hold that the use of DNA constituted an unconstitutional search under the Fourth Amendment. The four-member dissent in *King*, composed of Justices Scalia, Ginsburg, Sotomayor, and Kagan, noted that the majority sidestepped the constraints of the "search incident to arrest" doctrine—the same doctrine the majority applied in *Riley*, as described above.[117] A search incident is "justified by the interests in officer safety and in preventing evidence destruction."[118] The routine collection of DNA, however, does not serve either purpose. Instead, the majority appeared to craft a creative solution: treating DNA like any other routine booking procedure.[119] The only

108. Kaye, *supra* note 83, at 535; *King*, 569 U.S. at 469 (Scalia, J., dissenting).
109. *King*, 569 U.S. at 466.
110. *Id.* at 470.
111. *Id.* at 454; Ram, *supra* note 59, at 1385.
112. Dery, *supra* note 91, at 135, 141; *King*, 569 U.S. at 455.
113. Ram, *supra* note 59, at 1385; *King*, 569 U.S. at 453.
114. *King*, 569 U.S. at 472 (Scalia, J., dissenting).
115. *Id.* at 471 (Scalia, J., dissenting); Bradley, *supra* note 79.
116. *King*, 569 U.S. at 471 (Scalia, J., dissenting).
117. *Id.* at 468–69; Riley v. California, 573 U.S. 373 (2014).
118. *Riley*, 573 U.S. at 374.
119. *See* Dery, *supra* note 91, at 153–54 ("[S]hoehorning DNA swabs into a discussion of photography strained not only the Court's Fourth Amendment analysis, but also its credibility.").

difference between DNA and fingerprints or photographs, the Court reasoned, is DNA's unparalleled ability to achieve almost completely accurate identification.[120] Furthermore, DNA can also exonerate individuals wrongly accused of crimes.[121]

The *King* decision appears to be an odd exception to the Fourth Amendment, but it may not be so different from recent Fourth Amendment jurisprudence. With the emergence of new surveillance technologies, the Court often struggles to apply precedent while preserving the spirit of the Fourth Amendment.[122] Unlike other recent decisions, however, *King* shortsightedly declined to provide Fourth Amendment protections to a technology that would inevitability become more pervasive over time. Since the Court's decision in 2013, law enforcement has continued to routinely collect DNA from arrestees, convicted offenders, and crime scenes.[123] As this Note will show, *King* failed to consider important facets of DNA collection.

B. *Fourth Amendment Doctrine Shifts with Evolving Technology, Producing Narrow Holdings and Collective Harms*

DNA collection demonstrates the ongoing dilemma within Fourth Amendment doctrine. First, DNA collection, like many surveillance technologies, is constantly evolving and advancing. Second, the Court's highly fact-specific inquiry produces narrow holdings, which fail to address contemporary law enforcement activities. Finally, the exclusive focus on individual rather than collective harms has left millions of individuals, many of whom are minorities, vulnerable to future surprise querying of their DNA profiles.

1. The Evolving and Advancing Nature of Surveillance Technology Poses a Unique Challenge to Fourth Amendment Doctrine

First, DNA collection illustrates the difficulties of fitting new technology into existing legal doctrines. The Court based its decision in *King* partly on the assumption that CODIS loci from the "junk regions" are unrelated to information regarding genetic disease or predisposi-

120. *King*, 569 U.S. at 436.

121. *Id.* at 442; Ram, *supra* note 59, at 1385.

122. Hu, *supra* note 2, at 1831.

123. *CODIS-NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/M5S3-AWTE].

tions.[124] As noted above, however, researchers in the field believed that non-protein coding regions have at least some association with genetic disease and genetic predispositions.[125] Since the *King* decision in 2013, researchers have found that the development of the uterus and opposable thumbs derive from sequences found in non-coding regions.[126] Recently, in 2019, researchers found a link between mutations in the noncoding region and autism.[127] This steadily increasing body of knowledge demonstrates that a Supreme Court decision founded upon the theory of "junk" DNA may be far from the scientific reality.[128]

Although the Supreme Court was incorrect in equating DNA from the noncoding regions to nothing more than junk, the actual privacy implications of information derived from these regions are disputed.[129] Noncoding DNA may provide guidance for enhancing therapies, but it may not raise the same host of privacy concerns associated with DNA from coding regions. Yet, even if little private information could be derived directly from the twenty CODIS loci (thirteen at the time of *King*) used to create a DNA profile, information from the coding regions is accessible to law enforcement through other databases.

In recent years, law enforcement has utilized direct-to-consumer (DTC) DNA databases like 23andMe and Ancestry.com, as well as publicly accessible databases, to investigate and solve crimes. Most notably, in 2018, law enforcement used GEDmatch to solve the Golden State Killer case.[130] Using DNA taken from the scene of a crime years back, law enforcement created a single nucleotide polymorphism (SNP) pro-

---

124. *See King*, 569 U.S. at 445 ("The CODIS loci are from the nonprotein coding junk regions of DNA, and 'are not known to have any association with a genetic disease or any other genetic predisposition.'").

125. Dery, *supra* note 91, at 147.

126. Daniel Bastardo Blanco, *Our Cells Are Filled with 'Junk DNA' — Here's Why We Need It*, DISCOVER (Aug. 13, 2019), https://www.discovermagazine.com/health/our-cells-are-filled-with-junk-dna-heres-why-we-need-it [https://perma.cc/P3Q5-Y3AK]; Strickland, *supra* note 99.

127. *See* Jian Zhou, Christopher Y. Park, Chandra L. Theesfeld, Aaron K. Wong, Yuan Yuan, Claudia Scheckel, John J. Fak, Kevin Yao, Yoko Tajima, Alan Packer, Robert B. Darnell & Olga G. Toryanskaya, *Whole-Genome Deep-Learning Analysis Identifies Contribution of Noncoding Mutations to Autism Risk*, 51 NATURE GENETICS 973 (2019), https://www.nature.com/articles/s41588-019-0420-0 [https://perma.cc/BA5S-LBX8].

128. *See King*, 569 U.S. at 442.

129. Jake Buehler, *The Complex Truth About 'Junk DNA*,' QUANTA MAGAZINE (Sep. 1, 2021), https://www.quantamagazine.org/the-complex-truth-about-junk-dna-20210901/ [https://perma.cc/Y9R8-TKVW].

130. Ayesha K. Rasheed, *Personal Genetic Testing and the Fourth Amendment*, 2020 U. ILL. L. REV. 1249, 1261 (2020) (citation omitted). GEDmatch sits "downstream" from DTC DNA databases like 23andMe and Ancestry.com. *About GEDmatch*, GEDMATCH, https://www.gedmatch.com/about-us [https://perma.cc/9AJM-9U3T]. Essentially, after an individual receives her results and a file with raw genetic data from the DTC company, she can then upload her file to GEDmatch and compare her results to others in the database. *How It Works*, GEDMATCH, https://www.gedmatch.com/how-it-works [https://perma.cc/7PRM-AEMD].

file and uploaded it to GEDmatch.[131] The profile eventually led to an ex-cop named Joseph DeAngelo.[132]

An SNP profile differs greatly from an STR profile traditionally created and uploaded to CODIS. In the CODIS context, a profile is made from STRs in twenty locations on the genome.[133] In comparison, a GEDmatch profile uses SNPs containing information from around 600,000 locations on the genome.[134] SNPs can reveal far more personal medical information and family relations (which is why many people use the websites in the first place).[135] As noted above, the CODIS loci used to create an STR profile for CODIS were specifically selected for their location on the genome, which was thought to reveal far less about the individual.

In *King*, the Court reasoned that only records relating to identification would be collected and stored under the Maryland Act.[136] In the Golden State Killer case, law enforcement sidestepped this process entirely. In *King*, law enforcement initially collected DNA at the scene of the crime and created a DNA profile using the thirteen CODIS loci.[137] After Mr. King committed a different crime, his DNA was collected and matched to the previously-created DNA profile.[138] In comparison, in the Golden State Killer case, law enforcement created an entirely separate DNA profile using SNPs—a profile comprised of far more revealing genetic traits.[139]

The cost of the Golden State Killer method remains a barrier to widespread adoption. Creating an SNP profile is much more expensive than creating an STR profile for CODIS.[140] Recall, as Justice Alito said, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[141] With the rapid advance of technology, however, practical limitations begin to dissipate.

In 2018, a study aiming to understand the relationship between CODIS and DTC databases demonstrated that law enforcement is not

---

131. Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database*, ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695/ [https://perma.cc/YW2A-MRUK].

132. James W. Hazel & Christopher Slobogin, *'A World of Difference'? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 DUKE L.J. 705, 725–26 (2021).

133. Zhang, *supra* note 131.

134. *Id.*

135. *Id.*

136. *See King*, 569 U.S. at 444.

137. *Id.* at 445.

138. *Id.* at 435.

139. *See* Zhang, *supra* note 131.

140. Zhang, *supra* note 131.

141. *See* United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring).

necessarily restricted to this expensive, multistep SNP process.[142] An officer could simply use the information already uploaded to CODIS and then see if there are any hits on another database.[143] Initially, CODIS and commercial databases could not communicate with each other.[144] However, the study showed how to run a familial search using data from arrestee databases.[145] With the thirteen markers used for CODIS, researchers could link the data to individual profiles stored in DTC databases such as 23andMe with at least ninety percent accuracy.[146] Following the 2018 study, CODIS adopted seven more markers, greatly increasing the crossover between it and the recreational databases.[147] This study is important: it demonstrates that our initial understanding of CODIS profiles, and the underlying privacy concerns, are no longer subject to the parameters the Court relied on in justifying its permissive holding in *King*.

The Supreme Court's initial analysis of DNA was certainly dated at the outset. But even if the Court had given greater weight to the contemporary scientific understanding of non-coding DNA, it could not have predicted the later connection between CODIS and DTC databases. Evidently, the constantly evolving nature of technology is a particular challenge in the Fourth Amendment surveillance context.

2. The Court's Application of Fourth Amendment Doctrine Leads to Highly Fact-Specific, Narrow Holdings

Second, the Court's narrow holdings often have little application outside their specific sets of facts. The analysis in *King* is narrow: it specifically focuses on the Maryland law and the law's safeguards. As of 2018, thirty other states and the federal government have enacted DNA

142. *See* Jaehee Kim, Michael D. Edge, Bridget F.B. Algee-Hewitt, Jun Z. Li & Noah A. Rosenberg, *Statistical Detection of Relatives Typed with Disjoint Forensic and Biomedical Loci*, 175 CELL 175, 848, 848 (2018); *see also Computational Model Links Family Members Using Genealogical and Law-Enforcement Databases*, SCIENCEDAILY (Oct. 11, 2018), https://www.sciencedaily.com/releases/2018/10/181011143120.htm [https://perma.cc/6WR7-L4K2] [hereinafter SCIENCEDAILY].

143. *See* Kim, et al., *supra* note 142, at 848; *see also* SCIENCEDAILY, *supra* note 142.

144. *See generally* Kim et al., *supra* note 142; *see generally* SCIENCEDAILY, *supra* note 142.

145. SCIENCEDAILY, *supra* note 142 ("The key idea is that each STR marker is surrounded by SNPs that are typically inherited together with the STR. As a result, a person's genotypes for those SNPs can partially predict the genotype of the neighboring STR and vice versa. When these subtle correlations are accumulated across many STRs, it becomes possible to match an SNP profile with an STR profile.").

146. Kim et al., *supra* note 143, at 855.

147. *Id.*

arrestee laws,[148] many of which do not look like the statute addressed in *King*.[149]

The criteria and methods for DNA collection also differ between states. The Maryland law at issue in *King* is limited to specific serious offenses; the law authorizes the collection of DNA from an individual who is charged with a crime or attempted crime of violence or burglary.[150] At least seven states permit the collection of DNA for both felonies and certain misdemeanors.[151] For example, in Arizona, misdemeanors that qualify for DNA collection include "indecent exposure, public sexual indecency, and employment in prostitution."[152] Additional differences in state laws include the timing of the DNA analysis and the uploading of the DNA profile, as well as applicability to juveniles.[153]

Expungement practices also differ among states such that an individual's DNA profile may remain in the database even after her charges are dismissed. In some states, if the individual wishes to remove her DNA profile from the system, the onus is on her to request the removal, provided the law permits such expungements.[154] Given the difficulties associated with expungement generally, many individuals who are not convicted of a crime may remain in the database.[155]

Finally, in many states, DNA samples collected in the course of an investigation may be used for non-investigative purposes.[156] For example, in Massachusetts, under a broad, ambiguous umbrella of "humanitarian purpose," the director of the state DNA database may choose to provide identifiable DNA information to an individual or organization.[157] In Utah, state laws explicitly allow the disclosure of DNA information upon request to a "physician, physician assistant, psychologist,

148. *See generally* NAT'L CONF. OF STATE LEGISLATURES, DNA ARRESTEE LAWS (2018), https://www.ncsl.org/Documents/cj/Arrestee_DNA_Laws.pdf [https://perma.cc/57PC-K7KH].

149. *See* Maryland v. King, 569 U.S. 435, 445 (2013).

150. *Id.* at 443.

151. DNA ARRESTEE LAWS, *supra* note 148, at 4–8.

152. *Id.* at 4.

153. *Id.* at 4–8.

154. *Id.*

155. *See* ARIZ. REV. STAT. ANN. § 13-905(A) (2019); In Arizona, for example, the law allows for certain convictions to be "set aside" by the court, following the completion of probation or sentence and discharge. Set aside law essentially restores the individual's rights and releases her from "all penalties and disabilities resulting from conviction." *Arizona Restoration of Rights & Record Relief*, RESTORATION OF RTS. PROJECT (Mar. 11, 2020), http://ccresourcecenter.org/state-restoration-profiles/arizona-restoration-of-rights-pardon-expungement-sealing/#I_Loss_restoration_of_civilfirearms_rights [https://perma.cc/82PH-HHF5].

156. BARRY STEINHARDT, *Privacy and Forensic DNA Data Banks*, *in* DNA & THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 176, 177 (David Lazar, ed., 2004).

157. *Id.*

certified social worker, insurance provider or producer, or a government public health agency . . . ."[158]

In his 2004 analysis of state DNA laws, Barry Steinhardt notes that forty-eight states permit access to DNA records "for vaguely defined law enforcement purposes that go well beyond the limited use for the purpose of identification."[159] In his view, such permissive state laws "implicitly [allow] genetic tests for physical and mental traits or for predisposition to disease or 'criminality.'"[160] At the time of Steinhardt's writing, there was not a single state law that provided for the destruction of the samples after completing the DNA profile.[161]

In *King*, the Court determined that the processing of Mr. King's DNA sample "did not intrude on his privacy in a way that would make his DNA identification unconstitutional."[162] However, unlike a search for weapons or evidence on an arrestee, the start of a DNA search may not be as clear as the Court suggests.[163] Upon collection—beyond the physical intrusion of a buccal swab search—an arrestee becomes subject to the risk that her DNA may be provided to a physician or insurance provider or used for "humanitarian purposes."[164] As a result, the "search" may begin well before the analysis of the DNA for identification purposes. Consequently, the privacy concerns around the use of DNA are not simply cabined to the information that can be gleaned from the twenty CODIS loci; the privacy concerns may extend to the use of DNA generally, including coding DNA.

In *King*, the Court specifically addressed the Maryland DNA Collection Act in a narrow holding: a search using a buccal swab to obtain a defendant's DNA following a serious offense is reasonable under the Fourth Amendment.[165] Other states' practices evidently reach beyond *King's* narrow holding. Though highly fact-specific, narrow holdings are common in Fourth Amendment cases, they often fail to reflect the reality of, or constrain, law enforcement activities.

---

158. UTAH CODE ANN. § 63g-2-202 (West 2021); *accord* UTAH CODE ANN. § 63g-2-302 (West 2021); *see also* STEINHARDT, *supra* note 156, at 177.

159. STEINHARDT, *supra* note 156, at 178.

160. *Id.*

161. *Id.*

162. *See* Maryland v. King, 569 U.S. 435, 464 (2013).

163. *Id.* at 463–64. The Court in *King* does address whether the initial buccal swab inside the arrestee's cheek constitutes a search. However, the Court focuses on the physical aspects of the search, rather than the information that can be gleaned from the buccal swab, ultimately determining that it merely "involves a brief and minimal intrusion with virtually no risk, trauma, or pain." *Id.* at 438.

164. MASS. GEN. LAWS ANN. ch. 22E, § 10(d) (West 2022); *accord* STEINHARDT, *supra* note 156, at 176.

165. *King*, 569 U.S. at 465.

3. A Collective Harm: DNA Surveillance Database

Third, current Fourth Amendment doctrine fails to address collective harms arising out of mass surveillance. While the routine collection of DNA can have great societal benefits, serving to both combat crime and exonerate those who have been wrongfully convicted, it may also engender societal-level harms. Today, there are over eighteen million profiles in CODIS from arrestees and convicted offenders, a disproportionate share of whom are people of color.[166] An additional one million profiles obtained from crime scenes are in CODIS as well.[167] As it continues to accrue DNA profiles, CODIS begins to look more like widespread surveillance disproportionately impacting certain already disadvantaged groups.

With "small data," like the collection of a person's movements in *Jones*, the investigation begins with the individual.[168] Conversely, with collection programs such as those used by the National Security Agency (NSA),[169] large amounts of data are gathered into a database, which often provides information on individuals who are tangential to a criminal investigation. Authorities may query that database at a later date.[170] Professor Hu describes this process as maintaining a "digital dossier" of files on the entire population that is available to the government at a moment's notice.[171] Unlike ordinary criminal investigations, which focus on one individual, this process treats each person in society as if they may one day be a suspect.[172]

The collection of DNA appears to serve both individual and societal purposes. The collection begins when the individual is arrested and law enforcement determines whether the individual may have a prior history or be connected to any unsolved crimes.[173] However, it does not end there. Even when an individual is not convicted, her profile may remain in the database and can be queried later.[174]

Leaving the profile in the database poses an additional problem. While the criminal justice system is premised on the notion that each person is innocent until proven guilty, the current collection practices suggest that even if a person is not a criminal today, they may become

166. *CODIS-NDIS Statistics*, *supra* note 123.

167. *Id.*

168. Hu, *supra* note 2, at 1843; *see* United States v. Jones, 565 U.S. 400, 403 (2012).

169. Hu refers to this as "big data," however, big data tends to refer to a much larger collection of data—different from the surveillance tools the NSA employs. Hu, *supra* note 2, at 1843.

170. *Id.*at 1843–44.

171. *Id.* at 1845.

172. *See id.*

173. *CODIS-NDIS Statistics*, *supra* note 123; *see* Maryland v. King, 569 U.S. 435, 441 (2013).

174. *See King*, 569 U.S. at 440.

one tomorrow.[175] DNA collection and storage, like other surveillance programs, have become effortless. And unlike the routine collection of fingerprints, the information can connect the arrestee to her family members.[176]

An NSA surveillance program has evident differences from the CODIS database. The collection of metadata, providing information on who you talk to and when, is different from the twenty CODIS loci that are gathered to create a DNA profile for the database. But even if the information gathered is minimal, the societal awareness that the government is routinely collecting and building a DNA database may have significant implications, especially when the collection overrepresents minority populations.[177]

There are no current, complete, and available data regarding the racial and ethnic backgrounds of the people whose DNA profiles are stored in CODIS.[178] However, people of color are disproportionately stopped, searched, and arrested, often due to racial stereotyping, racial profiling, and the over-policing of communities of color.[179] In 2017, 27.2% of individuals arrested were Black or African American and 18.1% were Hispanic or Latino.[180] Furthermore, data from 2001 demonstrated that one in three Black men and one in six Latino men were likely to experience imprisonment in their lifetime, as compared to one in seventeen white men.[181] Now, considering that DNA collection occurs not just upon imprisonment, but upon arrest for certain crimes, one can imagine just how expansive CODIS is.[182] Given the over-policing of communities and the racial stereotyping that many people of color experience, around two-thirds of all adult men of color either have a DNA profile in the database or can be found through a familial search.[183] In one statis-

175. *See* Hu, *supra* note 2, at 1845–46.

176. *CODIS-NDIS Statistics*, *supra* note 123.

177. *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("[A]wareness that the government may be watching chills associational and expressive freedoms.").

178. *See* Erin Murphey, *DNA in the Criminal Justice System: A Congressional Research Service Report* (*from the Future)*, 64 UCLA L. REV. DISCOURSE 340, 367 (2016).

179. *See id.* at 354; Rachel Cox, *Unethical Intrusion: The Disproportionate Impact of Law Enforcement DNA Sampling on Minority Populations*, 52 AM. CRIM. L. REV. 155, 160 (2014).

180. *2017 Crime in the United States*, FBI: UCR (Sept. 24, 2018), https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/tables/table-43/#overview [https://perma.cc/BH8S-CZRH].

181. Thomas P. Bonczar, *Prevalence of Imprisonment in the U.S. Population, 1974-2001*, U.S. DEP'T JUST. (Aug. 2003), https://www.bjs.gov/content/pub/pdf/piusp01.pdf [https://perma.cc/7ET8-X86B].

182. *See* Jeremy Gruber, *Forensic Genetics: A Global Human Rights Challenge*, OPEN SOC'Y FOUNDS. (Mar. 21, 2012), https://www.opensocietyfoundations.org/voices/forensic-genetics-a-global-human-rights-challenge [https://perma.cc/M5Y4-V366]; Andrea Roth, Maryland v. King *and the Wonderful, Horrible DNA Revolution in Law Enforcement*, 11 OHIO STATE J. CRIM. L. 295, 308 (2013). Roth notes that about thirty percent of individuals arrested for a felony in California are never convicted. *Id.*

183. *See* Cox, *supra* note 179, at 160–61.

tic from 2011, Black Americans accounted for forty percent of the CODIS database[184] but only fourteen percent of the U.S. population.[185]

Ultimately, while the *King* decision considers the collection of arrestee DNA as nothing more than routine fingerprinting, that analogy is less applicable when the identification process is used to create a database that can link not only to an arrestee, but also to her family members. At a certain point, a routine booking procedure becomes routine surveillance.

III. DNA COLLECTION IS JUST ANOTHER SURVEILLANCE TECHNIQUE

Scholars have long sought to remedy the problems underlying Fourth Amendment jurisprudence considered in Part I. Many advocate for a new Fourth Amendment test to address emerging surveillance technologies, echoing the Court's solution in *Katz*.[186] Others place the solution within the purview of Congress.[187]

This Note does not purport to solve all the problems with Fourth Amendment jurisprudence. Scholars have been proposing various solutions for decades.[188] During this time, the Court has continued to create carve-outs and exceptions to the doctrine, and no legislative solution has sufficiently addressed growing privacy concerns.[189] As this Note

---

184. Roth, *supra* note 182, at 308; Jason Silverstein, *The Dark Side of DNA Evidence*, NATION (Mar. 27, 2013), http://www.thenation.com/article/173554/dark-side-DNA-evidence [https://perma.cc/HF2V-RPGU].

185. Christine Tamir, Abby Budiman, Luis Noe-Bustamante & Lauren Mora, *Facts About the U.S. Black Population*, PEW RSCH. CTR. (Mar. 25, 2021), https://www.pewresearch.org/social-trends/fact-sheet/facts-about-the-us-black-population/ [https://perma.cc/P44P-FUTP].

186. *See, e.g.*, Rachel Levinson-Waldman, *Hiding in Plain Sight, a Fourth Amendment Framework Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 549 (2017); Hu, *supra* note 2, at 1819.

187. *See e.g.*, Hu, *supra* note 2, at 1878.

188. The *Katz* "crisis" is not necessarily new. Lewis Katz (no relation to the *Katz* case), for example, in 1990, suggested a shift in jurisprudence to "focus on a new class of searches called 'intrusions.'" Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 555 (1990). In recent years, Hu, for example, has suggested a "cybersurveillance nonintrusion test" drawn upon values implicitly suggested by the Court in previous cases. Hu, *supra* note 2, at 1889–90. The test shifts the focus from individual harms to societal harms—a solution to address the harms of mass surveillance. Other solutions have ranged from "a return to a textually-based interpretation of the Fourth Amendment, to the passage of a constitutional amendment explicitly establishing a right to privacy, to the creation of a federal agency to monitor privacy, to an appeal to *Lochner*-era formalist interpretation." Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 138–39 (2004).

189. *See* Kamin, *supra* note 188, at 118. Kamin writes that there is no overarching privacy legislation; instead, there is an "alphabet soup" of federal legislation providing protection to varying degrees to address different privacy concerns. *Id.* Examples include the Video Privacy Protection Act (VPPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). *Id.* Kamin writes, "[r]ather than creating an omnibus privacy act, Congress has reacted to high-profile privacy concerns by attempting to remedy specific privacy threats." *Id.*

demonstrates, many of the concerns related to DNA collection arise out of generally unclear Fourth Amendment doctrine.

A distinct solution for DNA collection is not necessary. DNA is clearly a law enforcement surveillance technique and ought to be treated as such. Regardless of whether the Court adopts a new test or whether Congress provides a new framework, Fourth Amendment doctrine should analogize DNA collection to CSLI, GPS-tracking devices, or cell phones. In other words, DNA should fall within the protective provisions of Fourth Amendment jurisprudence.

Section III.A argues that DNA should fall within the protective provisions of the Fourth Amendment. Section III.B provides a framework for assessing DNA collection, demonstrating the application of the Fourth Amendment to DNA collection.

A. *DNA Collection Should Fall Within the Protective Provisions of the Fourth Amendment*

In *King*, the Court declined to include DNA collection within the scope of Fourth Amendment protections, essentially distinguishing DNA collection from other surveillance technologies like cell phones, CSLI, and GPS-tracking devices. Current DNA collection practices, however, raise many of the same concerns—concerns that the Court itself has expressed. Law enforcement use of DNA is ultimately like the use of other surveillance technologies and ought to be treated as such.

Information derived from DNA is personal and private, like information gathered from other surveillance technologies. The *Riley* Court wrote that cell phones are so pervasive "that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[190] DNA is not simply *like* an important feature of human anatomy—it *is* an important part of human anatomy. It contains a wealth of information unique to each individual and can reveal personal information about the individual and her family members. Incidentally, personal information found on cell phones—such as search history of medical symptoms and "frequent visits to WebMD"—is considered too private to be accessed by law enforcement as a routine part of arrest.[191] While *Riley* precludes law enforcement from accessing an arrestee's search history on WebMD, *King* allows law enforcement to freely access the raw data revealing an arrestee's gene expression, which includes the risk of developing the same diseases the arrestee was researching on WebMD.[192]

190. Riley v. California, 573 U.S. 373, 385 (2014).
191. *Id.* at 395–96.
192. *See id.*; Maryland v. King, 569 U.S. 435, 435 (2013).

Additionally, the Court has rejected proposed limitations to law enforcement searches as insufficient to protect individual privacy. In *Riley*, the government advocated for restricting law enforcement's search of the cell phone; instead of unbridled access to the phone, law enforcement would be required to remain within the bounds of information pertaining to the crime, the arrestee's identity, and officer safety.[193] The Court rejected the government's arguments, believing such parameters would "impose few meaningful constraints on officers."[194] The categories would provide officers with access to a broad spectrum of information, and officers would not know where to locate certain specific information prior to a search.[195]

In contrast to *Riley*, the *King* Court argued that law enforcement could limit the scope of a search of DNA.[196] This may be easier for DNA than for a cell phone, since the twenty CODIS loci are specifically selected, and law enforcement does not have to search through the genome to find information that pertains to identity. Even if the search can be restricted, however, the government may choose *not* to restrict the search, as demonstrated by state laws and the use of direct-to-consumer DNA databases.[197] The search of DNA goes far beyond the use of the twenty CODIS loci for identification purposes.

Furthermore, Fourth Amendment doctrine is malleable.[198] But protections guarding against law enforcement's use of DNA versus cell phones or CSLI should not depend upon whether the Court understands the science or appreciates the privacy concerns. As Justice Gorsuch noted, one's Fourth Amendment protections should not rise or fall with the "personal sensibilities" of the justices.[199]

Finally, one could argue that DNA ought to be entitled to greater protections than other privacy intrusions resulting from other technologies, but this misses the point. Views of surveillance, privacy, and different technologies differ from person to person—and especially among judges. One individual may have no qualms with her DNA being readily available to law enforcement, while another may view it as the greatest possible invasion of her privacy. The same range of reactions applies to the prospect of law enforcement searching cell phones; while one individual may think a cell phone is more private than DNA, another may advocate for greater protection for DNA than cell phones. Each poses privacy concerns, which vary individually.

---

193. *Riley*, 73 U.S. at 399.
194. *Id.*
195. *Id.*
196. *King*, 569 U.S. at 465.
197. STEINHARDT, *supra* note 156, at 177 (discussing non-identification uses of DNA).
198. *See* Kamin, *supra* note 188, at 139.
199. *See* Carpenter v. United States, 138 S. Ct. 2206, 2269–70 (2018) (Gorsuch, J., dissenting).

This is precisely the problem that a solution to Fourth Amendment doctrine should address—a solution that accounts for these value judgments. Advocating for greater protections for DNA merely leaves us in the current value-laden approach, which failed to protect DNA from government intrusion in *King*. Even if the Court's jurisprudence sufficiently protects DNA, what about the next technology?

B. *A Fourth Amendment Framework for DNA Collection*

As discussed above, this Note does not purport to create a new *Katz* test or provide a framework for navigating a new *Katz* moment. However, this Note provides a set of guiding principles to rethink how DNA collection ought to be assessed within the protective provisions of the Fourth Amendment. Application of the Fourth Amendment to DNA collection should consider several factors, including: (1) use of DNA by non-law enforcement entities, (2) expungement procedures, (3) the timing of the collection, (4) the reason for the collection, and (5) warrant requirements.

First, there should be greater safeguards to ensure that DNA is limited to law enforcement use, rather than use by various entities for reasons as broad as "humanitarian purposes."[200] The *King* Court was careful in making the distinction between coding and non-coding DNA, as DNA from coding regions is more identifying, and thus generates greater privacy concerns.[201] Yet broad, multi-use state laws completely derail the Court's analysis. The Court determined that the "processing of [the] CODIS loci did not intrude on [Mr. King's] privacy in a way that would make his DNA identification unconstitutional," yet it failed to assess whether the use of the DNA beyond the processing of the twenty pre-determined CODIS loci would be an unconstitutional search.[202] Ultimately, if DNA is specifically collected to help law enforcement investigate crimes or identify suspects, it should be used for only these purposes.

In addition to limiting the scope of DNA's use, expungement procedures should also be strengthened. Except for thirteen states, including Maryland, most states do not provide for automatic expungement of the DNA profile if the charge does not lead to a conviction.[203] Expungement procedures are important. As discussed above, the CODIS database likely overrepresents people of color, many of whom may have been arrested without being convicted. Automatic expungement re-

200. MASS. GEN. LAWS ANN. ch. 22E, § 10(d) (West 2022); STEINHARDT, *supra* note 156, at 176.
201. *King*, 569 U.S. at 442–443, 445.
202. *Id.* at 437; Dery, *supra* note 91, at 136.
203. DNA ARRESTEE LAWS, *supra* note 148.

quirements would ensure that only those who are found guilty of a crime are added to CODIS.

Furthermore, as discussed in Section II.B.2, state laws differ as to when DNA collection may occur. Under the Maryland law addressed in *King*, DNA is collected at booking.[204] The DNA may not be analyzed or the profile uploaded, however, until after the first scheduled arraignment date.[205] Unlike Maryland, at least a handful of states begin the analysis and upload sooner. For example, in Colorado, law enforcement may analyze and upload a suspect's DNA profile when she is charged with a felony.[206] In Ohio, the law *requires* that DNA profiles be analyzed and uploaded no later than fifteen days after collection, which occurs during the booking process.[207]

One solution, unused by states today, is to prevent the collection and upload of DNA until after an individual is convicted of a crime.[208] This could also mitigate the addition of innocent individuals to the database. Shifting the timing of collection to conviction erases the fiction that DNA is used for identification purposes. This change may be merely cosmetic. The fact pattern of *King*, as well as various state laws, already erodes this fiction, as many states openly decline to use DNA for identification purposes.

Another solution would be to simply cease *routine* collection of DNA and allow collection only when the government articulates reasons as to why the individual may be connected to another crime, and why DNA may facilitate the investigative process. This reverses the current underlying assumption of DNA collection, which allows for collection based upon the charged crime and presumes the arrestee's propensity to commit prior crimes.

Again, this solution undermines the notion that DNA is used for identification rather than investigation. It also challenges the assumption that DNA collection is an appropriate tool to use without a higher showing of probable cause. Therefore, the simplest solution may be a warrant requirement. While the Court declined to apply the "search incident to arrest" doctrine in *King*, re-evaluating the warrant requirement may be essential, given our growing understanding of DNA collection since the *King* decision.

Ultimately, a solution tailored to DNA may mitigate some of the immediate concerns that arise when a police officer takes a buccal swab to the inside of an arrestee's cheek. With a growing database that continues to add more minority DNA profiles to the pool, a timely solution

---

204. *Id; King*, 569 U.S. at 435.
205. *King*, 569 U.S. at 435; DNA ARRESTEE LAWS, *supra* note 148.
206. DNA ARRESTEE LAWS, *supra* note 148.
207. DNA ARRESTEE LAWS, *supra* note 148.
208. *Id.*

is certainly imperative. However, addressing DNA collection separately from related Fourth Amendment concerns merely patches the problem and may not resolve the multifaceted issues with Fourth Amendment doctrine. The current permissibility of law enforcement's treatment of DNA is deeply embedded in Fourth Amendment jurisprudence. The solution, therefore, must start with the Fourth Amendment.

CONCLUSION

This Note has examined evolving interpretations of the Fourth Amendment and the U.S. Supreme Court's complex relationship with emerging and novel technologies, as animated by DNA collection. DNA does not fit neatly within traditional Fourth Amendment jurisprudence, but neither do most emerging technologies. Had the Court applied traditional doctrine in recent cases, law enforcement would currently be able to search arrestee's phones, track people's locations, and obtain their CSLI, all without a warrant.

DNA collection demonstrates the ongoing drawbacks of Fourth Amendment doctrine. The doctrine is unable to account for the evolving and advancing nature of surveillance technology. It relies on highly fact-specific inquiries and produces narrow holdings that fail to reflect the reality of, or constrain, law enforcement activities. Its focus on individual harms, rather than the collective harm to society, leaves many without recourse. Regardless of which solution to the Fourth Amendment doctrine conundrum is ultimately adopted, DNA collection ought to fall within the doctrine's protections and provide a model of what such protections may look like.

There are important implications for treating DNA like other surveillance technologies. DNA plays an important role in criminal investigations and placing limits on collection could impede law enforcement efforts. But even though cell phones, GPS-tracking devices, and CSLI all enhance law enforcement's crime solving capabilities, the Court decided that their privacy intrusion often outweighs their benefit. In each case, the Court did not attempt to ban surveillance techniques; it simply extended the safeguards guaranteed under the Fourth Amendment. DNA is merely another *Katz* moment. With the evolving and advancing nature of surveillance technology, however, there will always be another moment. Fourth Amendment doctrine ought to account for such consistent shifts.