No. 14-885

IN THE

Supreme Court of the United States

GLENN JOSEPH RAYNOR,

Petitioner,

v.

STATE OF MARYLAND,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI
TO THE COURT OF APPEALS OF MARYLAND

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONER

JENNIFER LYNCH
Counsel of Record
LEE TIEN
HANNI FAKHOURY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jlynch@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

257466

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

Federal Cases

Cited Authorities

Cited Authorities

Page

Page

State Cases

State Statutes

Constitutional Provisions

Page

Other Authorities

Page

Page

Page

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has served as *amicus* in privacy cases before this Court, including in *Riley v. California*, 134 S. Ct. 2473 (2014), *United States v. Jones*, 132 S. Ct. 945 (2012), *National Aeronautics and Space Administration v. Nelson*, 131 S. Ct. 746 (2011), and *City of Ontario v. Quon*, 560 U.S. 746 (2010). EFF has also served as *amicus* in several cases considering the constitutionality of DNA collection and analysis. *See Maryland v. King*, 133 S. Ct. 1958 (2013); *People v. Buza*, 231 Cal. App. 4th 1446 (2014); *Haskell v. Harris,* 745 F.3d 1269 (9th Cir. 2014); *United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011).

INTRODUCTION

We cannot prevent inadvertently shedding our DNA. Of the billions of skin cells each human body possesses, we shed roughly "400,000 skin cells daily from all parts

1. Pursuant to Supreme Court Rule 37.2(a), *amicus* has provided timely notice to all counsel, and both parties consent to the filing of this brief. Pursuant to Supreme Court Rule 37.6, *amicus* states this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amicus* or its counsel made a monetary contribution to fund the preparation or filing of this brief. Web sites cited in this brief were last visited on February 13, 2015.

of the body,"[2] and we lose as many as 100 strands of hair.[3] Each skin cell or hair strand shed is a sample of our DNA, containing our entire genetic makeup—private and intensely personal information that maps who we are, where we come from and who we will be. It can tell us where in the world our ancestors came from, who we are related to, our physical characteristics, and whether we are likely to get a host of genetically-determined diseases. Researchers have theorized DNA may also determine race, intelligence, criminality, sexual orientation, and even political ideology.[4]

The Fourth Amendment's central concern is with "giving police officers unbridled discretion to rummage at will among a person's private effects." *Arizona v. Gant*, 556 U.S. 332, 345 (2009). This "creates a serious and recurring threat to the privacy of countless individuals." *Id.* To minimize such discretion, warrantless searches are *per se* unreasonable, subject only to a few "jealously and carefully drawn" exceptions. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971). No exception applies here.

---

2. Mark Barash, *et al.*, *The Use of Adhesive Tape for Recovery of DNA from Crime Scene Items*, J Forensic Sci 2010 1, 7, http://www.academia.edu/5997288/The_Use_of_Adhesive_Tape_for_Recovery_of_DNA_from_Crime_Scene_Items_The_use_of_adhesive_tape_for_recovery_of_DNA_from_crime_scene_items.

3. Hair Loss, *American Academy of Dermatology*, https://www.aad.org/dermatology-a-to-z/diseases-and-treatments/e---h/hair-loss.

4. Erika Check Hayden, Ethics: Taboo Genetics, *Nature* (Oct. 2, 2013), http://www.nature.com/news/ethics-taboo-genetics-1.13858; Lizzie Buchen, Biology and ideology: The anatomy of politics, *Nature* (Oct. 24, 2012), http://www.nature.com/news/biology-and-ideology-the-anatomy-of-politics-1.11645.

The Maryland Court of Appeals decision failed Fourth Amendment scrutiny by (1) ignoring the government's initial collection of Raynor's DNA and minimizing the "intrusiveness" of the actual "search" by focusing solely on the extraction of a 13-loci CODIS DNA profile;[5] and (2) minimizing the significant privacy interests implicated by unfettered police discretion to rummage through a person's most personal and sensitive possession—his DNA. The result was a failure to heed this Court's warning that Fourth Amendment rules "must take account of more sophisticated systems that are already in use or in development." *Kyllo v. United States*, 533 U.S. 27, 36 (2001).

This Court should grant *certiorari*.

ARGUMENT

I. *CERTIORARI* IS NECESSARY TO MAKE CLEAR THE FOURTH AMENDMENT PROHIBITS THE WARRANTLESS COLLECTION AND SEARCH OF INADVERTENTLY SHED GENETIC MATERIAL

The Maryland court's ruling—that the Fourth Amendment fails to protect against the warrantless collection and search of inadvertently shed genetic material—presages a future in which every person's DNA could be collected, sampled and profiled, not only without individualized suspicion of wrongdoing but without a person's knowledge and despite his refusal to consent.

---

5. CODIS is the FBI's Combined DNA Index System, which "connects DNA laboratories at the local, state, and national level." *Maryland v. King*, 133 S. Ct. 1958, 1968 (2013).

A. The Warrantless Collection and Indefinite Retention of Raynor's DNA is an Unconstitutional "Seizure"

The Fourth Amendment prohibits unreasonable seizures. A "seizure" occurs when there is "some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Government interference with an individual's property rights is a seizure, even if the owner's privacy was not violated. *See Soldal v. Cook Cnty.*, 506 U.S. 56, 62-64, 68 (1992). One of the most crucial property rights is the right to exclude others. *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982).

Law enforcement collection of inadvertently shed genetic material is a seizure, and the wholesale, warrantless seizure of a person's genome eviscerates any property right a person has to exclude others from this data. The Maryland court, however, only recognized the state's *search* of "13 junk loci;" it failed to acknowledge the state must first *seize* the entire genome to extract these 13 loci. *Raynor v. State*, 99 A.3d 753, 761 (Md. 2014). And this seizure is not momentary; the state retains this DNA sample indefinitely, allowing it to repeatedly search the sample any time without a warrant. *See Varriale v. State*, 96 A.3d 793, 799 (Md. App. 2014) (protections of Maryland's DNA Collection Act only apply to persons who "have given DNA samples *after being charged with or convicted of certain enumerated crimes*" (emphasis added)). Thus *all* the data in that sample is in the government's possession and outside the individual's control, and nothing prevents the state from testing the sample again. Unsurprisingly,

some states do precisely that; California retests samples after a familial search of its database identifies a partial match.[6]

Courts have recognized the indefinite retention of computer files—even files obtained via search warrant—can become an unconstitutional "seizure" because it unreasonably interferes with a person's possessory interest in sensitive and personal data. *See, e.g., United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014) (retaining computer data and searching it after seizure for unrelated crime violated Fourth Amendment); *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam) (recognizing "over-seizing is an inherent part" of computer searches and necessitates "greater vigilance . . . in striking the right balance" between government and private interests); *United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009) (twenty-one day delay between seizing computer and securing search warrant violated Fourth Amendment). In these cases, the initial seizure was not the constitutional problem; often the government was authorized by search warrant to make and retain copies of the seized files. Rather the problem was the owner's inability to ultimately control subsequent uses of the once-private information. *See* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 711 (2010) ("[w]hen the government makes an electronic copy of data, it obtains possession of the data that it can preserve for future use").

---

6. *See Information Bulletin: DNA Partial Match (Crime Scene DNA Profile to Offender) Policy*, No. 2008-BFS-01, Cal. Dep't of Justice, (Oct. 27, 2008), http://ag.ca.gov/cms_attachments/ press/ pdfs/n1548_08-bfs-01.pdf.

The same concerns apply here; the government's collection and indefinite retention of a DNA sample that it can repeatedly analyze significantly interferes with a person's ability to control his private genetic material. *See United States v. Davis*, 690 F.3d 226, 245-46 (4th Cir. 2012) (recognizing a continuing privacy interest in DNA even when police already have "lawful possession of the DNA sample"). The Maryland court's ruling invites other police departments to retain any and all DNA they collect. This Court's intervention is therefore necessary to assess the constitutionality of this practice.

B. The Warrantless Search of Inadvertently Shed Genetic Material Is "Unreasonable" Under the Fourth Amendment

"'[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (citation omitted). Where, as here, a search is undertaken to "discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant." *Id.* (quotations omitted). The Maryland court's conclusion that no "search" occurred rests on inaccurate analogies to older cases involving primitive technologies and consequently ignores the significant privacy interest in genetic material.

1. Searches of Genetic Material Defy Easy Parallels to Earlier Cases Involving Less Revealing Technologies

The warrantless search of inadvertently shed genetic material necessarily requires the seizure and search of a person's entire genome and may occur without that

person's knowledge. Because this search allows access to private and sensitive genetic information, it defies easy parallels to prior Fourth Amendment cases. This Court, when faced with new technologies, has recognized the challenges in "assur[ing] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *See United States v. Jones*, 132 S. Ct. 945, 958 (2012) (Alito, J. concurring) (quoting *Kyllo*, 533 U.S. at 34). And, it has jettisoned the constraints of earlier cases to ensure that technology does not eradicate the Fourth Amendment. For example, in *Kyllo* this Court did not feel bound by earlier precedent in *California v. Ciraolo*, 476 U.S. 207, 213 (1986), when it found intimate details inside the home were protected even though police were able to "see" those details from a public street. *Kyllo*, 533 U.S. at 33.

This Court reaffirmed this principle last term when it unanimously rejected the government's "strained" attempt to analogize cell-phone searches to the searches of physical items—like a pack of cigarettes—which the Court had approved decades earlier. *See Riley*, 134 S. Ct. at 2491; *id.* at 2484–89 (discussing *United States v. Robinson*, 414 U.S. 218 (1973)). Automatically extending cases from a different era involving less intrusive and revealing technologies to novel contexts in the digital age ignores the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34.

Yet, rather than recognize the challenges posed by the surreptitious collection and search of inadvertently shed genetic material, the Maryland court analogized the facts of this case to the voice sample addressed in *United States v. Dionisio*, 410 U.S. 1 (1973). *Raynor*, 99 A.3d at 761. But

genetic material can reveal far more about a person than a simple voice exemplar, and a government search of DNA is far more intrusive.

Given the sensitivity of DNA and the intrusiveness of testing, parallels to earlier cases involving less intrusive technologies are "strained." *See Riley*, 134 S. Ct. at 2491. Courts in the digital age must confront the technology before them, "take the long view, from the original meaning of the Fourth Amendment forward," and avoid the temptation to simply analogize to analog cases. *Kyllo*, 533 U.S. at 40.

2. Inadvertently Shed DNA Is Not Exposed to Others or Abandoned

The Maryland court's most critical mistake was finding Raynor "exposed to the public, albeit not to the naked eye, the identifying content of the genetic material he left on the armrests of the chair." *Raynor*, 99 A.3d at 766. This belief stems from *California v. Greenwood*, 486 U.S. 35 (1988), where this Court found no expectation of privacy in garbage left on the side of the road for collection because it was "common knowledge" that garbage was readily accessible to others and left for the "express purpose of conveying it to a third party, the trash collector." 486 U.S. at 40. Although the Maryland Court stated it was not addressing whether Raynor "abandoned" any privacy interests in his DNA, the practical import of its conclusion is that once DNA is left behind for others to pick up, it loses all Fourth Amendment protection. *See Raynor*, 99 A.3d at 765 n.11.

But DNA is nothing like trash. One does not consciously leave behind DNA for others to pick up or scientifically analyze. Raynor's own experience confirms this: when asked, he refused to give police a DNA sample and yet, like all humans, he could not help but leave one behind inadvertently on the chair when he left. *Raynor*, 99 A.3d at 756.

Critically, the Maryland court did not properly determine whether Raynor knowingly "abandoned" or "exposed" his DNA. Abandoning property must be a knowing and voluntary act. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 227-28 (1973) (consent to a search must be "voluntary" and not the "product of duress or coercion, express or implied"). Raynor did not knowingly and voluntarily leave his genetic material behind, meaningfully "abandon" it, or "expose" it to the public. *See Florida v. Riley*, 488 U.S. 445, 455 (1989) (O'Connor, J., concurring) (noting if public rarely travels overhead at a particular altitude, the area is not "knowingly expose[d]" to the public). Allowing the Maryland court's decision to stand places everyone at risk of having DNA collected and analyzed because we cannot avoid shedding DNA wherever we go.

3. *Maryland v. King* Does Not Control the Outcome of this Case

The Maryland court relied on this Court's decision in *King* to hold no search occurred in this case. *Raynor*, 99 A.3d at 762, 767. But this case is quite unlike *King*. *See Davis*, 690 F.3d at 250, n.29 (distinguishing facts of *King*).

First, because *King* involved the collection of DNA from an entire class of individuals—pre-trial arrestees—there was no risk of unfettered officer discretion. The Fourth Amendment's warrant requirement is intended to eliminate "general searches" and ensure "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 195-196 (1927). In *King*, lack of police discretion helped justify the warrantless and suspicionless collection and analysis of an arrestee's DNA. *King*, 133 S. Ct. at 1969-70. However, the collection and DNA testing that occurred here was based solely on an officer's decision to search Raynor's genetic material. Thus, it posed very real risks of limitless discretion absent in *King*. *See Davis*, 690 F.3d at 249-50 (unlike cases where DNA is collected "from everyone in [a] certain group of persons," DNA "specifically sought as a result of police suspicions that [a person] was involved in [a crime], and based on some quantum of proof amounting to less than probable cause" creates risk of arbitrary use of government power, so the need for a warrant is its highest).

Second, *King* involved DNA collection from arrestees, individuals who have "diminished" privacy rights because they are in custody, and there is probable cause to suspect they have committed a crime. *Bell v. Wolfish*, 441 U.S. 520, 557 (1979). Raynor, however, was not charged with any crime when his DNA was collected and was presumed innocent. While Raynor was ultimately arrested and charged, this cannot "eradicate his expectation of privacy" in his DNA at the time it was first collected. *See Davis*, 690 F.3d at 244.

Third, *King* addressed DNA collected directly from an arrestee's body with the arrestee's knowledge of

the collection. *See King*, 133 S. Ct. at 1969 (warrantless searches permissible in circumstance where "individual is already on notice" because of "conditions of his release . . . that some reasonable police intrusion on his privacy is to be expected") (citing *Samson v. California*, 547 U.S. 843 (2006)). Here, because there was no physical invasion of Raynor's body, he could not have known his DNA was being collected. More critically, when given the opportunity, he expressly did not consent to the collection.

Finally, the state had no need to use DNA to "identify" Raynor. In *King*, the Court described the government interest as "the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody." *King*, 133 S. Ct. at 1970. *King* emphasized that interests in identification are clearly connected to the "routine administrative procedure[s] at a police station house incident to booking and jailing the suspect." *Id.* at 1970 (quoting *Illinois v. Lafayette*, 462 U.S. 640, 643 (1983) (quotations omitted)). These interests were not implicated for Raynor because he was not booked or in police custody. The officers knew exactly who he was because he came voluntarily to the station after being identified as a suspect by the victim. *Raynor*, 99 A.3d at 755. The sole purpose of seizing and searching his DNA was to link him to an unsolved crime.[7]

7. Another significant difference between inadvertently shed genetic material and the DNA collected in *King* is that none of the protections in Maryland's DNA Collection Act or the regulations promulgated under the Act apply to DNA extracted from shed genetic material. *See Varriale*, 96 A.3d at 799 (protections of Maryland's DNA Collection Act apply solely to "persons who have given DNA samples *after being charged with or convicted of certain enumerated crimes*" (emphasis added)); Code Md. Reg.

As *King* does not control the outcome of the case, the Maryland court's decision should be reviewed.

II. THE COLLECTION AND SEARCH OF INADVERTENTLY SHED DNA IMPLICATES SIGNIFICANT PRIVACY INTERESTS

That a person "has diminished privacy interests does not mean that the Fourth Amendment falls outside of the picture entirely," and when "privacy-related concerns are weighty enough, a search may require a warrant, notwithstanding the diminished expectations of privacy[.]" *Riley*, 134 S. Ct. at 2488 (quoting *King*, 133 S. Ct. at 1979). With DNA—arguably our most sensitive and personal information—privacy concerns are "weighty enough" to require a warrant.

Fourth Amendment intrusion is measured not solely by physical trespass or inaccurate analogies to primitive techniques like fingerprinting, but by the impact of the government's entrance into what society considers a private sphere. *See Katz v. United States*, 389 U.S. 347, 353 (1967) ("the Fourth Amendment protects people—and not simply 'areas'" and "cannot turn upon the presence or absence of a physical intrusion into any given enclosure"). As *Riley* noted, the quantity and quality of information revealed to the government has constitutional significance. *See Riley*, 134 S. Ct. at 2489 (because "[c]ell phones differ in both a quantitative and a qualitative sense from other

---

29.05.01.02.A(1) (regulations do not apply to "evidentiary, suspect, and forensic samples otherwise legally obtained, whether by search warrant, court order, consent, or other method"). This includes the Act's protections against unfettered police access to the sample, limitations on the use of the sample, and procedures for expungement.

objects that might be kept on an arrestee's person[,]" a warrantless search incident to arrest was prohibited).

Numerous judges have recognized the threat to privacy posed by ever-expanding DNA collection and analysis. *See, e.g., King*, 133 S. Ct. at 1989 (Scalia, J. dissenting) (noting the "vast (and scary) scope" of majority's holding); *Raynor*, 99 A.3d at 771 (Adkins, J., dissenting) (DNA "is immensely personal and private, and deserves the staunchest protection under the Fourth Amendment"); *People v. Buza*, 231 Cal. App. 4th 1446, 1468 (2014) ("DNA contains an extensive amount of sensitive personal information" (citation omitted)); *State v. Medina*, 102 A.3d 661, 682 (Vt. 2014) (DNA "provide[s] a massive amount of unique, private information about a person that goes beyond identification of that person"); *Haskell v. Harris,* 669 F.3d 1049, 1079 (9th Cir. 2012) (W. Fletcher, J., dissenting) ("DNA testing constitutes a greater infringement on privacy than fingerprinting"); *United States v. Mitchell*, 652 F.3d 387, 424 (3d Cir. 2011) (Rendell, J., dissenting) (courts "should not be blind to the potential for abuse" with DNA analysis, and "concerns are legitimate and real, and should be taken into account"); *United States v. Kincade*, 379 F.3d 813, 842 n.3 (9th Cir. 2004) (Gould, J., concurring) ("the advance of science promises to make stored DNA only more revealing in time").

Three aspects of the expanding use of DNA technology are relevant to the Court's analysis: (1) the breadth and depth of private information available in DNA, (2) the clear trend toward cheaper and faster DNA analysis, driving the expansion of DNA collection and use, and (3) the very real threats to liberty posed by excessive collection. Taken

together, failing to protect against warrantless collection and search of inadvertently shed genetic material will usher in a future where DNA may be collected from any person at any time, entered into and checked against DNA databases, and used to conduct pervasive surveillance.

A. DNA Contains a Person's Most Private and Personal Information

A DNA sample—whether taken from a cheek swab or the armrest of a chair—contains a person's entire genetic makeup. This private and intensely personal information can reveal where our ancestors came from, who we are related to, whether we are likely to suffer from genetically-determined diseases, and possibly even our behavioral tendencies and sexual orientation.[8]

Profiles extracted from DNA samples have their own privacy concerns. Although Maryland does not allow familial searches on DNA collected from arrestees or those convicted of a crime,[9] this restriction does not apply to DNA collected from other sources.[10] Familial searches

---

8. *See supra* n. 4.

9. Md. Code Pub. Safety § 2-506(d).

10. *See* Stephen Mercer and Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. Ann. Surv. Am. L. 639, 679, n. 267 (2014) (noting director of Maryland DNA database "expressly limited the ban on familial searching *to DNA samples from arrestee and convicted offenders*." (emphasis added)). At least four other states expressly authorize such searches and use the 13 CODIS loci to conduct them. *See Familial Searching*, FBI, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/familial-searching.

can turn family members into "genetic informants" on each other. In Louisiana, a rape victim provided her DNA to help convict her rapist, but law enforcement used it instead to convict her brother of other crimes.[11] Familial searching also leads to false positives; researchers analyzing California's familial search protocol discovered recently that, because the protocol uses only limited data, there is "a substantial probability" of error—that a more distant relative such as a first cousin will be falsely identified as a first-degree relative such as a full sibling.[12] This means there is a high risk of turning immediate family members into targets for further investigation.

Familial searching disproportionately impacts minorities because criminal databases contain disproportionally more minority DNA.[13] If familial searching were conducted on a mass scale, as many as 17% of African-Americans could be identified through DNA profiles already in CODIS compared to only 4% of Caucasians.[14] This disproportionate representation leads

---

11. Mercer, *supra* note 10, at 640.

12. Rori Rohifs, *et al.*, *The Influence of Relatives on the Efficiency and Error Rate of Familial Searching*, PLOS One (Aug. 14, 2013), http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0070495.

13. *See Criminal Justice Fact Sheet*, NAACP, http://www.naacp.org/pages/criminal-justice-fact-sheet.

14. *See* Henry T. Greely, *et al.*, *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. Med. & Ethics 248, 259 (2006). CODIS has increased from about 4 million offender profiles in 2006 to more than 11.5 million today, so this percentage could now be much higher. *See CODIS Brochure*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis_brochure; *CODIS—*

to a "roughly two orders of magnitude higher" rate of false identification among the African-American population.[15]

Data aggregation—combining CODIS data with other publicly available genetic data—creates additional privacy risks. Tens of thousands of humans have had their genomes completely sequenced, and over a million have had high-resolution scans for genetic variants.[16] These numbers are increasing rapidly as the costs of sequencing decline.[17] Combining CODIS information with other genetic data[18] will make it possible to infer a person's physical traits or propensity for disease from his profile, because the alleles in a CODIS profile are linked[19] to specific regions within our DNA that influence physical traits or disease predispositions. Access to a profile and information about

---

NDIS Statistics, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/ codis/ndis-statistics.

15. Rohifs, *supra* note 12.

16. *See* Genomes by the Thousand, *Nature* (Oct. 28, 2010), http://www.nature.com/news/2010/101027/pdf/4671026a.pdf.

17. *Id.*; *DNA Sequencing Costs*, National Human Genome Research Institute, http://www.genome.gov/images/content/cost_genome.jpg (graph showing sequencing costs declining from $100 million in 2001 to less than $10,000 today).

18. Public sources for genetic data include the many online genetic genealogy databases and public health sources such as the National Institutes of Health's GenBank, "an annotated collection of all publicly available DNA sequences." *See GenBank Overview*, Nat'l Center for Biotech. Info., Nat'l Insts. of Health, http://www.ncbi.nlm.nih.gov/genbank/.

19. "Linked" in the genetic sense, meaning co-inherited with high probability.

the profile owner's relatives would, if any near relatives had their full genomic data in public databases, enable inferences about the profile owner's genetic makeup, including any disease-causing variant that lies in the third of the human genome co-inherited (roughly within 50 million base pairs) with a CODIS marker.

Researchers recently engaged in similar data aggregation to re-identify anonymized genetic samples—determining not just the name of a sample's owner but also his entire family.[20] Those researchers concluded that, "data release, even of a few markers, from one person can spread through deep genealogical ties and lead to the identification of another person who might have no acquaintance with the person who released his genetic data."[21] Although DNA profiles currently lack the Y-chromosome information the researchers used for re-identification, some states re-test offender DNA samples for Y-STR type once a familial search of its database identifies a partial match.[22]

---

20. Gymrek, *et al.*, *Identifying Personal Genomes by Surname Inference*, 339 Science 321, 322 (Jan. 18, 2013), http://data2discovery.org/dev/wp-content/uploads/2013/05/Gymrek-et-al.-2013-Genome-Hacking-Science-2013-Gymrek-321-4.pdf.

21. *Id.* at 224.

22. *Information Bulletin: DNA Partial Match (Crime Scene DNA Profile to Offender) Policy*, Cal. Dept. of Justice (Oct. 27, 2008)), http://ag.ca.gov/cms_attachments/press/pdfs/n1548_08-bfs-01.pdf. The FBI is exploring including Y STR and mitochondrial DNA in CODIS to determine patrilineal and matrilineal relationships. *See CODIS—The Future*, FBI, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis_future.

These risks will only increase as more genetic data becomes publicly available, more research is conducted on that genetic data, and the number of alleles included in a CODIS profile increases—which the FBI is considering.[23]

Sloppy policing, systemic DNA lab problems,[24] and even the increasing sensitivity of DNA testing tools have led to false identifications that can only occur if an innocent person's profile is already in a database. In San Jose, Lukis Anderson spent five months in jail after a database search linked his DNA to DNA found on the fingernails of a murder victim—although Anderson had been hospitalized when the murder occurred.[25] In Sacramento, Shawn Ponce was falsely arrested based on his DNA and jailed for five days for two crimes he could not have committed.[26] In England, David Butler spent eight months in jail after a database search falsely matched his DNA to that found on a murder victim—despite evidence establishing his

---

23. *See Planned Process and Timeline for Implementation of Additional CODIS Core Loci*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/planned-process-and-timeline-for-implementation-of-additional-codis-core-loci.

24. *See, e.g.,* DOJ OIG, *Audit of Compliance with Standards Governing combined DNA Index System Activities at the County of Santa Clara District Attorney's Crime Laboratory*, Audit Report GR-90-12-004 (Sep. 2012), http://www.justice.gov/oig/reports/2012/g901 2004.pdf.

25. Henry Lee, *How Innocent Man's DNA Was Found at Killing Scene*, SF Gate (June 26, 2013), http://www.sfgate.com/crime/article/How-innocent-man-s-DNA-was-found-at-killing-scene-4624971.php.

26. *See United States v. Ponce*, Mag.No. 07-00215-DAD (E.D. Cal. 2007), SW 07-2000-KJM (E.D. Cal. 2007), Mag.No. 07-0199 (C.D. Cal. 2007).

innocence.[27] Another British citizen was falsely accused of murdering a woman in Italy based solely on DNA.[28]

These concrete harms can only occur when innocent persons' DNA is collected and retained. *See King*, 133 S. Ct. at 1989 (Scalia, J., dissenting). And these false matches will only increase if this Court allows the continued warrantless, discretionary collection of inadvertently shed genetic material.

B. As the Cost of DNA Processing Drops, the Government Is Already Expanding Its Collection and Use of DNA

Collection, sharing and analysis of DNA profiles has increased significantly as technological advances, reduced costs, and policy changes enable even the smallest local police department to create and maintain its own DNA database.[29] And the result will be expanded warrantless DNA collection and analysis. *See Kincade*, 379 F.3d at 872 (Kozinski, J., dissenting) (without limits on DNA collection, "it's hard to see how we can keep the database from expanding to include everybody").

---

27. *See* Hannah Barnes, *DNA Test Jailed Innocent Man for Murder*, BBC (Aug. 31, 2012), http://www.bbc.co.uk/news/science-environment-19412819.

28. Linda Geddes, *DNA Super-Network Increases Risk of Mix-Ups*, New Scientist (Sep. 5, 2011), http://www.newscientist.com/article/mg21128285.500-euro-dna-treaty-risks-false-positives.html.

29. Joseph Goldstein, *Police Agencies Are Assembling Records of DNA*, N.Y. Times (June 12, 2013) http://www.nytimes.com/2013/06/13/us/police-agencies-are-assembling-records-of-dna.html.

With surveillance, reduced costs and increased efficiency are often detrimental to privacy. The Court recognized this in *Jones* when it considered the constitutionality of tracking a car via a GPS device for 28 days. Almost thirty years earlier, this Court held there was no expectation of privacy in public, secure in the fact the technique was so costly it was used only in limited circumstances. *See e.g., United States v. Knotts*, 460 U.S. 276, 283-84 (1983) (dismissing concerns over constant surveillance by finding "reality hardly suggests abuse" and reserving right to consider "dragnet-type law enforcement practices" when they occur) (quotations omitted). But in *Jones*, five justices expressed concern that technologies like GPS, which make "available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," could "alter the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations and citation omitted); *see also id.* at 963 (Alito, J., concurring) ("availability and use of . . . new devices will continue to shape the average person's expectations about . . . privacy"). The same concerns were present in *Riley*, where this Court found a cell phone "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 134 S. Ct. at 2491.

The concerns about GPS technologies and the prevalence of cell phones making government surveillance cheaper and easier apply equally to DNA. When forensic DNA testing began 30 years ago, testing was expensive

and required a blood sample. Labs needed large amounts of biological evidence from a crime scene to develop a DNA profile.[30] Analyzing DNA continued to be costly twenty years ago, when several states and the FBI began maintaining DNA indexes for law enforcement purposes.[31] Today, however, new technologies "make it possible to sequence the whole exome or genome of a person at a price that is affordable for some health-care systems."[32] A 2010 report prepared for the U.S. Department of Defense concluded that with improved technology "DNA sequencing costs will no longer be a factor limiting personal human genomics technologies."[33]

The monetary and practical costs of processing DNA samples to obtain a profile have also decreased. The federal government has invested substantial funds to develop Rapid DNA analyzers—portable machines about the size of a laser printer that can be used by non-scientists outside a lab.[34] These machines can produce a DNA profile

30. Mercer, *supra* note 10 at 646.

31. *See, e.g., CODIS Brochure*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis_brochure (FBI's National DNA system established in 1994); *see also The $100 Genome: Implications for the DoD*, JASON (The MITRE Corporation), at 2 (Dec. 15, 2010), www.fas.org/irp/agency/dod/jason/hundred.pdf (noting that the first attempts to sequence the human genome—a project started in 1990 and not completed until 2003—cost approximately $300 million).

32. Carla G van El, *et al.*, *Whole-genome sequencing in health care*, 21 European J. Human Genetics 580-84 (2013), http://www.nature.com/ejhg/journal/v21/n1s/full/ejhg201346a.html.

33. *See The $100 Genome* at 2, *supra* note 31.

34. *See* Jennifer Lynch, *Rapid DNA: Coming Soon to a Police Department or Immigration Office Near You*, EFF, (Jan. 6, 2013),

in 50 minutes or less for as little as $100 per sample[35] and are already used by law enforcement in Florida and Arizona.[36] With newer, more sensitive testing technology, police no longer need large quantities of genetic material; they "can collect and analyze trace amounts of 'touch' DNA from surfaces like doorknobs, steering wheels, or windows."[37]

Governments are also spending millions of dollars to expand other DNA collection and testing capabilities and to increase database capacity. In 2006, DOJ awarded a multi-year, multi-million-dollar contract to Unisys to develop "Next Generation CODIS," which would expand the "scalability and flexibility" of CODIS and include a "highly sophisticated search engine technology that will greatly accelerate the DNA matching process."[38] Since

---

https://www.eff.org/deeplinks/2012/12/rapid-dna-analysis. Records are available at https://www.eff.org/file/36203#page/2/mode/1up.

35. Portable DNA Analyzer, NEC, http://www.nec.com/en/global/solutions/biometrics/products/portable_dna_analyzer.html.

36. *See* IntegenX, *White Paper: The Case for Rapid DNA* (May 2012), http://integenx.com/wp-content/uploads/2012/05/The-Case-for-Rapid-DNA.pdf; Revolutionary DNA Testing Instruments Now Available to DPS Detectives, Arizona Dep't of Public Safety (May 13, 2014), http://www.azdps.gov/Media/News/View/?p=477.

37. Mercer, *supra* note 10 at 646.

38. *See* Press Release, *FBI Contracts with Unisys for Development and Deployment of Next-Generation Combined DNA Index System*, Business Wire (Oct. 19, 2006), http://www.businesswire.com/news/home/20061019005514/en/FBI-Contracts-Unisys-Development-Deployment-Next-Generation-Combined.

then, DOJ has been rolling out improvements to CODIS,[39] including "expanding CODIS capabilities in terms of DNA match technologies" and kinship searches.[40] DOJ also plans to link CODIS data to the extensive biometric and biographic data stored in its vast Next Generation Identification database.[41]

DNA collection and its attendant risks will only increase as more agencies create and build out existing local under- or unregulated DNA databases,[42] encouraged by the fact that DNA profiles generated outside of the FBI's strict regulations cannot be entered into CODIS.[43] The convenience and speed of Rapid DNA may further increase these risks. Once officers can use the machines to collect and process DNA from a squad car, doing so could become a routine part of traffic stops. Given the current uncertainty surrounding DNA collection laws, it is

---

39. *See generally Exhibit 300: Capital Asset Summary: FBI Combined DNA Index System (CODIS)*, UII 011-000002501, Dept. of Justice, (Aug. 8, 2012), https://it-2013.itdashboard.gov/investment/exhibit300/pdf/011-000002501.

40. *Id.; see also CODIS—The Future*, FBI, http://www.fbi.gov/about-us/lab/codis/codis_future (noting re-architecture of CODIS will allow it "to include additional DNA technologies" such as Y-STR and mtDNA, both of which can definitively determine kinship along paternal and maternal lineages).

41. Valerie Evanoff, FBI Next Generation Identification (NGI) DNA Study, Global Identity Summit (Sept. 17, 2014) http://www.biometrics.org/bc2014/presentations/Wed_1819_Evanoff_1540.pdf.

42. *See, e.g.,* Goldstein, *supra* n. 29 (describing Orange County, California's database).

43. *See FAQs on the CODIS Program and the National DNA Index System*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet.

unclear what standards would govern the use and prevent the abuse of these tools, including the collection of DNA with little or no suspicion of criminal activity.

Courts did not need to think about privacy interests in DNA when it was costly and difficult to analyze. That is no longer true. Just as we cannot hide our faces in public or participate in everyday life without leaving electronic footprints, we cannot hide our DNA; we leave skin cells wherever we go. To limit government DNA-based surveillance we must limit governmental collection and use of our shed DNA.

CONCLUSION

Warrantless collection and search of inadvertently shed genetic material is another step toward a future of limitless and lawless DNA collection, retention and analysis. This Court should grant *certiorari* and reverse course.

Respectfully submitted,

Jennifer Lynch
Counsel of Record
Lee Tien
Hanni Fakhoury
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jlynch@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

Dated: February 18, 2015