No. 12-207

IN THE

Supreme Court of the United States

STATE OF MARYLAND,

Petitioner,

v.

ALONZO JAY KING,

Respondent.

ON WRIT OF CERTIORARI TO THE COURT OF APPEALS OF MARYLAND

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

JENNIFER LYNCH
Counsel of Record
LEE TIEN
HANNI FAKHOURY
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94110
(415) 436-9333
jlynch@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation

245438

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

TABLE OF CONTENTS

Table of Contents

Page

TABLE OF CITED AUTHORITIES

Page

FEDERAL CASES

Cited Authorities

Page

Cited Authorities

Page

STATE CASES

Cited Authorities

Page

FEDERAL CONSTITUTIONAL PROVISIONS

FEDERAL REGULATIONS AND RULES

STATE STATUTES AND LEGISLATIVE MATERIALS

LAW REVIEW ARTICLES

Page

OTHER AUTHORITIES

Page

Page

Page

Page

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

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the information society. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. As part of its mission, EFF has often served as counsel or amicus in privacy cases, such as *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*, 130 S. Ct. 2619 (2010). EFF has also served as amicus curiae in several cases before federal and state courts considering the constitutionality of DNA testing of pretrial arrestees. *See Haskell v. Harris,* 669 F.3d 1049 (9th Cir. 2012), *reh'g en banc granted*, 686 F.3d 1121 (9th Cir. 2012); *United States v. Pool*, 621 F.3d 1213 (9th Cir. 2010), *vacated*, 659 F.3d 761 (9th Cir. 2011); *United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011); *People v. Buza*, 262 P.3d 854 (Cal. 2011), *granting review to* 129 Cal.Rptr.3d 753, 197 Cal. App. 4th 1424 (2011).

---

1. Pursuant to Supreme Court Rule 37.3(a), amicus states that petitioner and respondent have filed letters with the Clerk granting blanket consent to the filing of amicus briefs. 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 intended to fund the preparation or submission of this brief.

INTRODUCTION

Our DNA contains our entire genetic makeup—our most private information about who we are, where we come from and who we will be. DNA can be used to identify us in the narrow and proper sense of that word—"who is that?"—but it also tells the world who we are related to, what we look like, and how likely we are to get specific diseases. This Court must protect this sensitive genetic material by prohibiting the warrantless collection of DNA from arrestees.

SUMMARY OF ARGUMENT

The State of Maryland, like 27 other states and the federal government,[2] collects DNA without a warrant from people merely arrested for a crime—people who are presumed innocent and, therefore, not that different from the lawyers arguing this case or the justices deciding it. Maryland and supporting *amici* argue DNA collection is necessary to definitively identify an arrestee, but DNA profiles are not actually used to verify the arrestee's identity because the test cannot be used to verify a person's true identity *at the time of arrest*. Given this and the myriad other quick and effective identification tools already at Maryland's disposal—from fingerprints to palm prints to face recognition-capable photographs—it is clear that the true purpose of DNA collection from arrestees is entirely investigative.

---

2. *See* National Institute of Justice, *DNA Sample Collection From Arrestees*, http://nij.gov/topics/forensics/evidence/dna/collection-from-arrestees.htm (last visited January 30, 2013).

Maryland and *amici* also claim that DNA profiles contain no more data than a fingerprint. But DNA profiling naturally requires the seizure of a DNA sample that contains the arrestee's entire genome. As shown by the trend toward "familial" DNA searching, DNA profiles can tell who a person is related to and may be able to tell, when combined with other publicly available data, whether a person is more or less likely to have a given trait or get a specific disease. The breadth of information obtained by a mere fingerprint is not remotely comparable to that in DNA.

Thus, this Court must once again confront the "power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Technological advancements in the last twenty years have made it easier, cheaper, and faster to collect, process, search through, and analyze DNA and will "make stored DNA only more revealing in time." *United States v. Kincade*, 379 F.3d 813, 842 n.3 (9th Cir. 2004) (en banc) (Gould, J., concurring). Last year, in this Court's pivotal opinion in *United States v. Jones*, 132 S. Ct. 945 (2012), five justices recognized the power of technology to minimize and, in some cases eliminate, practical privacy protections by making mass data collection and surveillance not just possible, but routine. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring), 963 (Alito, J., concurring). As in *Jones*, this Court is forced to review searches that were not feasible twenty years ago, much less at the time the Fourth Amendment was drafted. In doing so, this Court must acknowledge the current and future backdrop of the search practices at issue here:

- The government must collect DNA samples to create DNA profiles, so any claim that the search and seizure does not implicate an individual's most private bodily information is false.

- The government retains both DNA profiles and samples almost indefinitely.

- The government repeatedly uses once-collected DNA profiles and samples for purposes unrelated to any one defendant's identity.

- The government has expanded, and will continue to expand, the scope of DNA sample and profile collection, both within and outside of the law enforcement context.

- DNA collection and analysis technology is rapidly advancing, making DNA searches less expensive and more efficient at determining information from an individual sample or profile.

If this Court were to adopt Maryland's arguments—that DNA may be collected without a warrant or individualized suspicion from people presumed innocent—people who are "just like everyone else . . . then it's hard to see how we can keep the database from expanding to include everybody." *Kincade*, 379 F.3d at 872 (Kozinski, J., dissenting). This Court should put an end to the inevitable expansion of warrantless DNA testing.

ARGUMENT

I. THE WARRANTLESS SEIZURE AND REPEATED SEARCH OF DNA TAKEN FROM MERE ARRESTEES IS UNCONSTITUTIONAL

Maryland's laws authorizing blanket DNA collection from individuals not yet convicted of a crime presage a future in which every person's DNA could be sampled and profiled without individualized suspicion.

Laws that give "police officers unbridled discretion to rummage at will among a person's private effects" violate the Fourth Amendment because searches that are not tied to finding evidence of the crime at issue "create[] a serious and recurring threat to the privacy of countless individuals." *Arizona v. Gant*, 556 U.S. 332, 345 (2009). 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, 455 (1971); *see also Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973); *Gant*, 556 U.S. at 338 (citing *Katz v. United States*, 389 U.S. 347, 357 (1967)).

Maryland has failed to show that warrantless DNA collection from arrestees falls within any of these "carefully drawn" exceptions, for three reasons. Maryland (1) relies on inapplicable Fourth Amendment exceptions to justify the search; (2) misinterprets the "intrusiveness" of the actual "search" by focusing on its physical aspects; and (3) ignores the significant and actual privacy interests involved.

A. The Fourth Amendment Prohibits Warrantless and Suspicionless DNA Collection from Arrestees

The Fourth Amendment only allows searches unsupported by individualized suspicion in "certain limited circumstances." *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 668 (1989); *see also Gant*, 556 U.S. at 338. Warrantless searches of arrestees have only been upheld in two, limited circumstances. Under the search incident to arrest exception to the Fourth Amendment, police may search an arrestee's person and the area within his immediate control in order to protect officers from hidden weapons, and prevent the destruction of evidence. *Gant*, 556 U.S. at 339 (citing *Chimel v. California*, 395 U.S. 752, 763 (1969)). Second, warrantless searches of arrestees has been authorized in the non-law enforcement context of prison security. *See Florence v. Bd. of Chosen Freeholders of County of Burlington*, 132 S. Ct. 1510 (2012); *Bell v. Wolfish*, 441 U.S. 520 (1979). Outside of these two circumstances, this Court has never approved of blanket, suspicionless searches of arrestees.

Maryland argues that this Court's decisions in *United States v. Knights*, 534 U.S. 112 (2001) and *Samson v. California*, 547 U.S. 843 (2006), upholding warrantless, suspicionless searches of probationers and parolees respectively, should also apply to searches of arrestees. *See* Brief of Petitioner at 12-13. In *Samson*, the Court upheld a suspicionless search of a parolee after employing a "totality of the circumstances" test "assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental

interests." *Samson*, 547 U.S. at 848 (quoting *Knights*, 534 U.S. at 118-19).

That test is inapplicable here, because mere arrestees are outside the scope of *Samson* and *Knights*. In both cases, this Court recognized that a person's status as a convicted felon is "salient." *Samson*, 547 U.S. at 848 (quoting *Knights*, 534 U.S. at 118). And in *Samson* this Court noted that "[p]robation is 'one point . . . on a continuum of possible punishments [and] [o]n this continuum, parolees have fewer expectations of privacy than probationers, because parole is more akin to imprisonment than probation is to imprisonment." *Samson*, 547 U.S. at 848, 850 (quoting *Knights*, 534 U.S. at 119). Arrestees are not and cannot be on this "continuum." As the Ninth Circuit has noted, "pretrial releasees are not probationers[;]" they "are ordinary people who have been accused of a crime but are presumed innocent." *United States v. Scott*, 450 F.3d 863, 871-872 (9th Cir. 2005) (citing *Ferguson v. City of Charleston*, 532 U.S. 67, 80 n. 15 (2001); *Griffin v. Wisconsin*, 483 U.S. 868, 874 (1987)).

Nor do the government interests that supported the suspicionless searches in *Knights* and *Samson* apply to searches of arrestees. In *Knights* and *Samson* the Court ruled that since both probationers and parolees have been *convicted*, the non-law enforcement interests of preventing recidivism and encouraging reintegration into society justify a suspicionless search. *Samson*, 547 at 853-54; *Knights*, 534 U.S. at 120-21. But collecting and searching DNA only serves the government's interest in law enforcement investigation. As one court has noted, "DNA profiles are neither necessary nor helpful for verifying who a person is at the time of arrest. Indeed, the fact that

DNA testing cannot be employed to verify a person's true identity at the time of arrest demonstrates that collection of a DNA sample at this time has another purpose." *People v. Buza*, 197 Cal. App. 4th 1424, 129 Cal. Rptr. 3d 753, 773 (2011), *review granted and opinion superseded*, 262 P.3d 854 (Cal. 2011). Rather, the only true purpose of DNA collection is to "detect evidence of ordinary criminal wrongdoing." *See City of Indianapolis v. Edmond*, 531 U.S. 32, 41, 44 (2000) (holding that a "program whose primary purpose is ultimately indistinguishable from the general interest in crime control" violated the Fourth Amendment). This purpose cannot support an exception to the Fourth Amendment's warrant requirement.

B. The Search at Issue is a Repeated Intrusion into a Person's Sensitive Genetic Information

Petitioner and supporting *amici* view DNA collection as a single, extended Fourth Amendment event, from initial swab to CODIS matching.[3] *See* Amicus Curiae Brief by the Los Angeles County District Attorney on Behalf of Los Angeles County at 9 ("accessing the DNA database is not a 'second search.'"). They then hang their arguments on the initial collection, arguing that its minimal physical discomfort fails to outweigh the state's interest in "identifying" the arrestee. But as the Maryland Court of Appeals and other courts have recognized, there

3. Petitioner, its supporting *amici*, and several cases have explained how DNA collection and processing operates—from collecting the DNA sample, processing that sample to obtain the 13-loci DNA profile, uploading the profile to state and federal level DNA databases, and then using the FBI's CODIS software to search for matches. *See, e.g.*, Petitioner's Brief at 3–4, 15–16; *Mitchell*, 652 F.3d at 399–401; *Boroian v. Mueller*, 616 F.3d 60, 65–66 (1st Cir. 2010).

are "two discrete and separate searches" involved in DNA collection. *King v. State*, 42 A.3d 549, 575 (Md. 2012); *see also United States v. Mitchell*, 652 F.3d 387, 406-7 (3d Cir. 2011) ("The second 'search' at issue is, of course, the processing of the DNA sample and creation of the DNA profile"). The state's analysis excludes any consideration of the arrestee's privacy interests in his DNA sample and profile and any consideration of his family members' privacy interests in their own genetic information.

"The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." *Schmerber v. California*, 384 U.S. 757, 767 (1966). Intrusion is measured not solely by the physical discomfort involved in the initial search but also by the breadth of the government's entrance into what was previously a private sphere. DNA searches involve "intrusion into the widest spectrum of human privacy." *United States v. Pool*, 621 F.3d 1213, 1232 (9th Cir. 2010) (Lucero, J., concurring), *opinion vacated* 659 F.3d 761 (9th Cir. 2011).

By disaggregating the multiple searches and seizures implicated by governmental DNA collection, it becomes clear that the privacy intrusion at issue is not limited to the initial physical extraction but instead stretches far beyond anything "reasonably related in scope to the circumstances which justified the interference in the first place." *New Jersey v. T.L.O.*, 469 U.S. 325, 341 (1985); *see also Kincade*, 379 F.3d at 873 (Kozinski, J., dissenting) ("it is important to recognize that the Fourth Amendment intrusion here is not primarily the taking of the blood, but seizure of the DNA fingerprint and its inclusion in a searchable database.").

Without question, the State's initial physical intrusion to collect a DNA sample from Mr. King—in this case, the buccal swab—is both a search and a seizure. *See Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 616-17 (1989) (breathalyzer and urine sample); *Cupp v. Murphy*, 412 U.S. 291, 295 (1973) (finger nail scrapings); *Schmerber*, 384 U.S. at 767-71 (blood). The extraction of Mr. King's DNA profile from that sample is a second search. *See Skinner*, 489 U.S. at 616 (recognizing that the "ensuing chemical analysis of the sample to obtain physiological data" is also a search). Placing his DNA profile into a state and national database and running the profile through CODIS for "hits" is another search. The same is true of every subsequent use of Mr. King's DNA profile for "matching," or running new DNA profiles against his to find a match. *See Kyllo*, 533 U.S. at 32 n.1 ("search" means "[t]o look over or through for the purpose of finding something; to explore." (quoting N. Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed.1989)); *see also United States v. Kriesel*, 508 F.3d 941, 956 (9th Cir. 2007) (B. Fletcher, J., dissenting) ("the warrantless 'search' permitted by the 2004 DNA Act extends to repeated searches of his DNA whenever the government has some minimal investigative interest.") (citing *Kincade*, 379 F.3d at 873 (Kozinski, J., dissenting)).

Moreover, the seizure of the DNA sample necessarily requires the seizure of a person's entire genome, raising another set of Fourth Amendment concerns. The Fourth Amendment was intended to prevent "general warrants" which allowed the government "to search and seize whatever and whomever they pleased" without judicial review or individualized suspicion. *Ashcroft v. al-Kidd*, 131 S. Ct. 2074, 2084 (2011). As a result, this Court has always

insisted that search warrants must "particularly describe the things to be seized" to ensure that when it comes to "what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (particularity "requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

Allowing the wholesale, warrantless seizure of a person's genome eviscerates the concept of particularity; it is in essence a "general search" of a person's genetic history. It is the equivalent of the government seizing and searching an entire computer, rummaging through all of its data— including data outside of the probable cause justification—to find one specific file. *See, e.g. United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam) ("that over-seizing is an inherent part of the electronic search process . . . calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."). Regardless of what the government does with the DNA sample and the limits it places on the sample's use, all the highly personal data in it is in the government's possession, and outside the individual's control.

By disaggregating the searches and seizures involved in DNA collection, it is clear that DNA collection serves investigatory rather than identification purposes and strays far beyond the government's stated need. Moreover,

as discussed below, each of these searches and seizures presents its own privacy concerns that far outweigh the government's stated or true purpose in collecting DNA. DNA collection from arrestees is no less a "police entitlement" than the vehicle search at issue in *Gant*, and "it is anathema to the Fourth Amendment to permit a warrantless search on that basis." *Gant*, 556 U.S. at 347.

C. The Privacy Interests Implicated by DNA Collection are Significant and Outweigh the Government's Interest in Investigating Crimes and Building Out DNA Databases

Maryland and its *amici* seek to diminish the privacy interests at stake by cabining them to the initial cheek swab and the thirteen loci currently contained in a DNA profile and then balancing those interests against the government's stated need to "identify" arrestees. However, this discounts the very real privacy interests implicated by the other searches and seizures outlined above. It also ignores the myriad other more effective methods Maryland already has at its disposal—from fingerprints[4] to palm prints[5] to face recognition-capable

4. *See* Maryland Dept. of Pub. Safety & Corr. Servs., *Keeping Communities Safe*, http://www.dpscs.state.md.us/initiatives/kcs/index_KCS_tech.shtml (last visited January 30, 2013) (noting that, using Maryland's new automated fingerprint system, "99% of criminal and non-criminal fingerprint submissions can now be matched digitally").

5. *Id.* (noting the new fingerprint system also "gives Maryland law enforcement a new palm search capability never before possible").

photographs[6] to the biographic information all arrestees must provide upon arrest—to identify arrestees.

As this Court explained in *Kyllo* "the rule [a court] adopt[s] must take account of more sophisticated systems that are already in use or in *development*." *Kyllo,* 533 U.S. at 36 (emphasis added); *see also Mitchell*, 652 F.3d at 424 (Rendell, J., dissenting) ("we should not be blind to the potential for abuse when assessing the legitimacy of [DNA collection]"). This Court must address three crucial aspects raised by the expanding use of DNA technology. These include (1) the sheer breadth and depth of information available in DNA, (2) the clear trend toward cheaper and faster DNA analysis, and (3) the increasing expansion of DNA collection and use throughout government and society as a whole. Taken together, these facts show that DNA collection allows the government to learn far more about its citizens than any other law enforcement technology previously addressed by the Court. If the Court does not scrupulously apply Fourth Amendment protections here, the continued evolution of DNA technology will usher in a future where DNA may be collected from any person at any time, entered into and checked against one or many DNA databases, and—as we discard our DNA wherever we go—used to conduct surveillance on a level far beyond anything currently possible with cameras, GPS, cell phone tracking or other such technology.

---

6. *See* Testimony of Jerome Pender, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, July 18, 2012, *available at* http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties (last visited January 30, 2013) (noting that Maryland is one of several states participating in a pilot face-recognition program with the FBI).

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

DNA—whether it is in the form of a full genetic sample or an extracted profile—can reveal an extraordinary amount of private information about a person. The court below recognized the "vast genetic treasure map" contained in the DNA sample collected and retained by the government. *King*, 42 A.3d at 577. Divided opinions from other courts have noted that DNA technology poses grave threats to personal privacy and expressed concerns about how the expansion of DNA collection portends a society in which every American's DNA will be sampled and profiled. *See Kincade*, 379 F.3d at 872 (Kozinski, J., dissenting) ("[i]f collecting DNA fingerprints can be justified [here], then it's hard to see how we can keep the database from expanding to include everybody."); *Mitchell*, 652 F.3d at 424 (Rendell, J., dissenting) ("we believe we should not be blind to the potential for abuse when assessing the legitimacy of government action. These concerns are legitimate and real[.]"). As one judge has noted, "the advance of science promises to make stored DNA only more revealing in time." *Kincade*, 379 F.3d at 842 n.3 (Gould, J., concurring).

a. The DNA Sample

The government cannot extract a DNA profile without first collecting a DNA sample that contains a person's entire genetic makeup—private and intensely personal information that maps, in the broadest sense, who we are, where we come from and who we will be. It can tell us which part of the world our ancestors came from; who we are related to; whether we are likely to get a host

of genetically-determined diseases, and possibly even behavioral tendencies and sexual orientation. *See Kincade*, 379 F.3d at 850 (Reinhardt, J., dissenting) (quoting Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 Tex. L. Rev. 49, 95-96 (1995) and noting that DNA sample can reveal "genetic defects, predispositions to diseases, and perhaps even sexual orientation").

Maryland, like other states that collect DNA samples, does not delete this genetic data when it creates a profile but instead retains it indefinitely. *See* Md. Code Pub. Safety §2-506(b).[7] The state and its *amici* try to discount the privacy risks inherent in retaining this data by arguing that Maryland's law restricts its use. *See* Petitioner's Brief at p. 15-16; Brief of the United States as Amicus Curiae Supporting Petitioner, at 22.[8] However,

---

7. Maryland does have a process for expunging DNA samples. *See* Md. Code. Pub. Safety §2-511. Automatic expungement occurs only after the initiation of the "criminal action" against the arrestee does not result in a conviction, is reversed or vacated, or the arrestee is granted an unconditional pardon. *Id.* at §2-511(a)(1). In other words, a criminal charge must be filed in order for the sample to be expunged automatically. In all other instances – including those where no charge is ever filed following arrest – the arrestee must take the effort to get the sample expunged. *Id.* at §§2-511(a)(2), (b).

8. Maryland laws already require the Director of the Crime Laboratory to "create a population data base comprised of DNA samples collected under this subtitle." Md. Code. Pub. Safety §2-509. The law requires the samples to be anonymized, but recent research suggests that is not possible. *See* Melissa Gymrek, *et al.*, *Identifying Personal Genomes by Surname Inference*, 339 Science 321, 322 (January 18, 2013).

as the Maryland Court of Appeals noted, "this does not change the nature of the search." *King*, 42 A.3d at 576.[9] It is anathema to the Fourth Amendment to allow an otherwise unconstitutional search and seizure solely because the government promises, for the time being, to avert its eyes to the treasure trove of data it has seized. And this Court has made it clear it "would not uphold an unconstitutional statute merely because the Government promised to use it responsibly." *United States v. Stevens*, 130 S. Ct. 1577, 1591 (2010).

b. The DNA Profile

Maryland and its *amici* argue that an arrestee's DNA profile contains no more information than a fingerprint. *See e.g.,* Petitioner's Brief at 19, Amicus Curiae Brief of Los Angeles County at 3-4, Amicus Brief of United States at 9. This analogy fails to recognize several important distinctions between the two—distinctions that judges have recognized make DNA profiles much more privacy invasive than fingerprints. *See Haskell v. Harris,* 669 F.3d 1049, 1079 (9th Cir. 2012) (Fletcher, J., dissenting), *reh'g en banc granted*, 686 F.3d 1121 (9th Cir. 2012) ("Even with today's technology, however, junk DNA reveals more information than a fingerprint.").

First, a fingerprint cannot reveal familial relationships. Yet, these relationships can already be inferred with a high degree of accuracy from the 13 loci the government

9. *See also Haskell*, 669 F.3d at 1079 (Fletcher, J., dissenting) ("Defendants claim that California does not currently conduct such familial searches on *arrestee* DNA profiles, but the possibility—even likelihood—that California will begin conducting such searches in the future remains.").

currently collects.[10] Although Maryland has banned familial searches for the time being,[11] four states expressly authorize such searches and use the 13 CODIS loci to conduct them.[12] Although the CODIS software has not yet been optimized for familial searching, the federal government and other jurisdictions can use it to generate partial matches.[13] The FBI is already considering expanding the CODIS core loci,[14] and once it does, familial relationships may be determined conclusively.

Familial searching disproportionately impacts certain groups in society because criminal DNA databases contain far more African American and Latino DNA than that of other ethnic and racial groups. Several researchers have determined that if familial searching is conducted on a mass scale, as much as 17% of the African American

10. *See* Fed. Bureau of Investigation, *Familial Searching*, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/familial-searching (last visited January 30, 2013).

11. Md. Code Pub. Safety §2-506(d).

12. *See*, *supra*, Fed. Bureau of Investigation, *Familial Searching*. These states include Colorado, California, Texas and Virginia.

13. *See generally*, Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 Stan. L. Rev. 751 (2011) (discussing various jurisdictions' approaches to partial matching and familial searching and differentiating between fortuitous and deliberate searching).

14. *See* Fed. Bureau of Investigation, *Planned Process and Timeline for Implementation of Additional CODIS Core Loci*, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/planned-process-and-timeline-for-implementation-of-additional-codis-core-loci (last visited January 30, 2013).

population in the United States (as opposed to only 4% of the Caucasian population) may be identified through the DNA samples already included in CODIS.[15] No parallel risk exists through mass fingerprint collection and search.

Data aggregation—the ability to combine CODIS profile data with other publicly available genetic data—adds in additional privacy risks. Currently, tens of thousands of humans have had their genomes completely sequenced and over a million have had high-resolution scans for genetic variants. And these numbers are increasing rapidly as the costs of sequencing decline. This means that a substantial, and ever growing, fraction of the population has a fourth degree or closer relative whose genetic information is available in public or private databases.

Although the alleles that make up a CODIS profile are non-coding and likely non-functional, they are linked[16] to specific functional regions within our DNA—regions that include genetic variants that influence phenotypic traits or predispose a person to specific diseases. By combining CODIS information with publicly available genetic data—whether from one of the many online genetic genealogy databases or from a source such as

---

15. Joyce Kim, *et al.*, *Policy implications for familial searching*, Investigative Genetics, November 2011, http://www.investigativegenetics.com/content/2/1/22 (citing Henry T. Greely, *et al.*, *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. Med. & Ethics 248, 262 (2006)) (last visited January 30, 2013).

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

the National Institutes of Health's GenBank[17] —it will be possible to infer, for example, a person's propensity for a particular trait or disease strictly from his CODIS profile. A person with access to a CODIS profile and information about the profile owner's relatives (whether inferred from the CODIS profile or from other biographical or genetic data) would, if any near relatives had full genome data in databases, be able to infer aspects of 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) of a CODIS marker.

That the government would engage in this kind of data aggregation and data mining is utterly predictable. Several federal agencies have centers devoted to analyzing publicly available data to look for trends and specific threats.[18] And researchers have recently engaged in similar data aggregation to re-identify anonymized genetic samples—determining not just the name of the

17. Nat'l Center for Biotech. Info., Nat'l Insts. of Health, *GenBank Overview*, http://www.ncbi.nlm.nih.gov/genbank/ (last visited January 30, 2013).

18. For example, new guidelines announced last year by the Office of the Director of National Intelligence allow the National Counterterrorism Center (NCTC) to obtain information from any government database, combine it with other publicly available data to conduct "pattern-based queries and analyses," and then share any of the original or resulting data with federal, state, local or tribal law enforcement, and also with foreign entities and individuals or entities not part of the government. *See* Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, Wall St. J., December 13, 2012, *available at* http://online.wsj.com/article/SB10001424127887324478304578171623040640006.html (last visited January 30, 2013).

person who submitted the sample in the first place but also his entire family—"in total . . . breach[ing] the privacy of nearly 50 individuals" from three original samples.[19] Those researchers concluded, "[t]his study shows 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." *Id.* Although DNA profiles do not currently contain Y chromosome information, which the researchers used for re-identification, California re-tests offender DNA samples for Y-STR type once a familial search of its database identifies a partial match.[20]

These risks will only increase as more and more genetic data becomes available, as more research is conducted on that genetic data, and as the number of alleles included in a CODIS profile increases.

c. Tangible and Intangible Harms

Government storage, use, and analysis of data after information has been collected create their own threats

---

19. Gymrek, *Identifying Personal Genomes by Surname Inference*, *supra* note 8 at 322.

20. Cal. Dept. of Justice, *CAL-DNA Data Bank Technical Procedures Manual* 27, October 17, 2008, *available at* http://www.aclunc.org/news/press_releases/asset_upload_file490_8577 (last visited January 30, 2013). The FBI is exploring including Y STR and mitochondrial DNA (to determine patrilineal and matrilineal relationships, respectively) in CODIS in the future. *See* Fed. Bureau of Investigation, *CODIS—The Future*, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis_future (last visited January 30, 2013).

to privacy and civil liberties. As privacy scholar Daniel Solove has noted, government collection and use of personal information—even personal information that is

> not particularly sensitive ... affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives."

Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745, 756-57 (2007). Government seizure of DNA also results in an individual's inability to control the dissemination of her sensitive, private data. *See e.g.*, Paul Ohm, *The Fourth Amendment Right to Delete*, 119 Harv. L. Rev. F. 10 (2005) (arguing that since "seizure" is about dispossession, an individual loses ability to delete information when the government has a copy of it).

The plaintiffs represented in *Haskell v. Harris*, a Ninth Circuit case that has been stayed pending the outcome of this case, show that almost anyone can be affected by warrantless DNA collection. Each had his or her DNA collected upon arrest. *Haskell*, 669 F.3d at 1066 (Fletcher, J., dissenting). Several were political activists and were arrested during demonstrations. *Id.* None of the plaintiffs was ever convicted of any charges, and in fact, after their DNA samples were taken, police dropped or

dismissed the charges against each of them. *Id.* Against two of the plaintiffs, no charges were ever filed. *Id.*[21]

As the plaintiffs in *Haskell* told the court, when the government collects DNA upon arrest without reason to believe the DNA is linked to a past crime, it is nothing more than an "intimidation tactic" that leaves a person afraid her DNA will falsely be matched to a sample obtained at a crime scene. *Haskell*, 669 F.3d at 1066 (Fletcher, J., dissenting). This is especially true when the arrest occurs in the context of a political demonstration. As Ms. Haskell told the court, this directly impacts an activist's "freedom of expression." *Id.*

Warrantless DNA collection can also lead to concrete harms because it increases risks from sloppy policing and systemic DNA lab problems.[22] In the U.K., David Butler was falsely accused of murder and spent eight months in jail solely because his DNA was in a database and was

---

21. This is typical in California, where the plaintiffs were arrested and where a third of the 300,000 people arrested for felonies each year are never convicted. Many arrestees are never even charged. Cal. Dep't. of Justice, *Crime in California 2011* 49, *available at* http://oag.ca.gov/sites/all/files/pdfs/cjsc/publications/candd/cd11/cd11.pdf (last visited January 30, 2013). Federal arrest and conviction rates follow a similar pattern. Mark Motivans, U.S. Dep't of Justice, *Federal Justice Statistics 2009 – Statistical Tables* 4, 18 (Dec. 2011), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/fjs09st.pdf (last visited January 30, 2013).

22. *See, e.g.,* William C. Thompson, *Tarnish on the "Gold Standard": Understanding Recent Problems in Forensic DNA Testing,* The Champion, Jan./Feb. 2006 at 10-12 (listing scandals); Annie Sweeny & Frank Main, *Botched DNA Report Falsely Implicates Woman*, Chi. Sun-Times, Nov. 8, 2004.

matched to DNA found on the murder victim despite the existence of other evidence clearly establishing he was nowhere near the victim when the murder occurred.[23] In Sacramento, California, Shawn Ponce was falsely arrested based on DNA and held in jail for five days for two bank robberies in Southern California that he could not have committed.[24] These risks would not have occurred if the defendants' DNA had not been in a database. As this Court noted long ago, "the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

Comparing DNA to fingerprints fails to recognize the essence of DNA collection and search. The intrusiveness of a fingerprint is limited to cataloging the pattern of loops and whorls on a person's finger. It cannot reveal the breadth and depth of information available to the state through DNA collection; nor can it lead to the tangible and intangible harms associated with DNA collection.

---

23. *See* Hannah Barnes, *DNA Test Jailed Innocent Man For Murder*, BBC, August 31, 2012, *available at* http://www.bbc.co.uk/news/science-environment-19412819 (last visited January 30, 2013).

24. *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).

2. Cheaper DNA Analysis Will Lead to More DNA Analysis

As technology improves, activities once deemed impossible become not just possible but cheap and efficient to conduct on a mass scale. With surveillance, however, cheapness and efficiency are not an unalloyed good; improved surveillance techniques pose serious privacy risks.

The Court recognized this last year in *Jones* when it found that 28 days of continuous and warrantless GPS surveillance of a car violated the Fourth Amendment. Before *Jones*, this Court could say that individuals had no reasonable expectation of privacy in public, secure in the fact that surveilling individuals was so costly and impractical that it occurred only for short periods of time when the government had a compelling reason to do so. *See e.g., United States v. Knotts*, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."); *Jones*, 132 S. Ct. at 963 (Alito, J., concurring in the judgment and noting that in the "pre-computer age," "[t]raditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."). As *Jones* itself and the FBI's actions after *Jones* demonstrate, GPS technology now makes such surveillance not just easier, but cheap and routine. *See Jones*, 132 S. Ct. at 948-49.[25]

25. *See* Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, Wall St. J., February 25, 2012, *available at* http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/ (last visited January 30, 2013) (noting that, according to FBI

Society faces the same set of issues for DNA technology. Twenty years ago, when several states and the FBI began maintaining DNA indexes for law enforcement purposes,[26] the cost of analyzing DNA was so great it did not factor into the lives of ordinary Americans.[27] This cannot be said today. The National Human Genome Research Institute at the National Institutes of Health notes "in a few years, the sequencing of a patient's entire genome will be an affordable standard diagnostic tool used in health care."[28] And a report prepared for the U.S. Department of Defense in 2010 predicted the cost to sequence an entire human genome would drop to $100 by

---

General Counsel Andrew Weissmann, "the court ruling prompted the FBI to turn off about 3,000 GPS tracking devices that were in use").

26. *See, e.g.,* Fed. Bureau of Investigation, *CODIS Brochure*, *available at* http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis_brochure (last visited January 30, 2013) (FBI's National DNA system established in 1994); Press Release, Cal. Dep't of Justice, *Brown Announces Elimination of DNA Data Bank Backlog* (Sept. 10, 2007), *available at* http://oag.ca.gov/news/press-releases/brown-announces-elimination-dna-data-bank-backlog (last visited January 30, 2013) (California established DNA database in 1990).

27. *See* JASON (The MITRE Corporation), *The $100 Genome: Implications for the DoD* 2 (Dec. 15, 2010), *available at* www.fas.org/irp/agency/dod/jason/hundred.pdf (last visited January 30, 2013) (noting that the first attempts to sequence the human genome—a project started in 1990 and not completed until 2003—cost approximately $300 million).

28. Nat'l Human Genome Research Inst., Nat'l Insts. of Health, *Overview of Genetic Testing*, https://www.genome.gov/10002335 (last visited January 30, 2013).

this year.[29] The report concluded that "third-generation" sequencing technology would mean that "DNA sequencing costs will no longer be a factor limiting personal human genomics technologies."[30]

The cost of processing DNA samples to obtain a DNA profile has also dropped dramatically. Records released by the Department of Homeland Security under the Freedom of Information Act show that the federal government has invested "substantial funds" to develop Rapid DNA Analyzers—machines about the same size as a laser printer that can extract a DNA profile in 90 minutes or less.[31] These machines can be used by non-scientists outside a lab and can process DNA for as little as $100 per sample.[32]

These profound cost decreases have made it easier—and in some cases routine—to collect, process and store genetic material in areas outside the law enforcement context. For example, the military mandates DNA collection from all members of the armed services.[33] Companies sell personal DNA testing kits to determine

---

29. *See generally The $100 Genome*, *supra* note 27.

30. *Id.* at 2.

31. *See* Jennifer Lynch, *Rapid DNA: Coming Soon to a Police Department or Immigration Office Near You*, Elec. Frontier Found., January 6, 2013, https://www.eff.org/deeplinks/2012/12/rapid-dna-analysis (last visited January 30, 2013). The Department of Homeland Security records are available at https://www.eff.org/file/36203#page/2/mode/1up (last visited January 30, 2013).

32. *Id.*

33. *See generally* Amicus Brief of Los Angeles County at 20.

health and ancestry information for as little as $99.[34] And state newborn genetic screening programs require blood collection from nearly all infants born in the United States.[35]

The reduced costs involved in DNA processing and advances in technology have also made it easier for companies and research institutions to make genetic data publicly available to anyone interested in searching

---

34. *See, e.g.,* 23andMe, https://www.23andme.com/(last visited January 30, 2013) (offering genetic tests for $99); Ancestry.com, http://dna.ancestry.com/offers/buyKit.aspx (last visited January 30, 2013) (offering genetic tests and access to "more than $10 billion international records" for $249); National Geographic, http://shop.nationalgeographic.com/ngs/product/genographic-kits/geno-2.0---genographic-project-participation-and-dna-ancestry-kit (last visited January 30, 2013) (testing "nearly 150,000 DNA markers that have been specifically selected to provide unprecedented ancestry-related information" for $199.95).

35. Newborn genetic screening is mandatory in 49 states, and almost all of the 4 million infants born in the United States each year are tested. *See* Michelle H. Lewis, *et al.*, *State Laws Regarding the Retention and Use of Residual Newborn Screening Blood Samples*, Pediatrics, March 28, 2011, at 704. Despite the important public health reasons for collecting and testing newborn blood, the programs have not been without controversy. *See* Emily Ramshaw, *DSHS Turned Over Hundreds of DNA Samples to Feds*, Texas Tribune, February 2, 2010, *available at* http://www.texastribune.org/texas-state-agencies/department-of-state-health-services/dshs-turned-over-hundreds-of-dna-samples-to-feds/# (last visited January 30, 2013) (noting that blood spots were turned over to "an Armed Forces lab to build a national and, someday, international mitochondrial DNA (mtDNA) registry" for forensic purposes).

it,[36] whether to discover information about their own ancestry,[37] to learn the identity of a biological parent,[38] or to conduct research on previously sequenced DNA to look for new insight on genetically-determined traits and heritable diseases.[39] Yet as these resources become more robust and more accessible, it also becomes much easier and much less costly to combine data from multiple databases and use it for purposes other than that for which it was originally intended.[40]

---

36. *See* Nat'l Human Genome Research Inst., *Free Online Tutorials Teach Anyone How to Use Genome Databases*, Nat'l Insts. of Health, http://www.genome.gov/27530225 (last visited January 30, 2013).

37. *See, e.g.,* Ysearch, http://www.ysearch.org (last visited January 30, 2013) (a free service offered by Family Tree DNA that allows a visitor to search his or her Y chromosome database by surname, genetic markers, and haplogroup); Sorensen Molecular Genealogy Foundation, http://www.smgf.org/pages/sorensondatabase.jspx (last visited January 30, 2013) (another free service that allows users to search their Y chromosome and mitochondrial DNA databases, which include "more than 100,000 DNA samples and family trees from men and women around the world.").

38. *See, e.g.,* Family Finder, http://www.familytreedna.com/landing/family-finder.aspx (last visited Jan. 30, 2013) (a service offered by Family Tree DNA that matches autosomal DNA with a DNA database to find biological relatives).

39. *See, e.g.,* Human Genome Resources, http://www.ncbi.nlm.nih.gov/projects/genome/guide/human/ (last visited January 30, 2013) (a free database of genetic information for biomedical researchers); UCSC Genome Bioinformatics Site, http://genome.ucsc.edu/ (last visited January 30, 2013) (another free database of genomic information with associated research tools).

40. *See* Gymrek, *Identifying Personal Genomes by Surname Inference*, *supra* note 8 at 321-324.

While some rules have been set up to regulate the collection, sharing and use of these DNA samples, the edges of these rules are hazy and changing.[41] And it has been shown in other sensitive data collection contexts that there is a high risk these treasure troves of data will be compromised or used for purposes beyond their original intention.[42]

Courts did not think about the privacy expectation in DNA when the cells we shed revealed nothing about us. That is no longer true. And just as we cannot hide our faces in public or enjoy many conveniences of everyday life without leaving electronic footprints, we cannot hide our DNA; we leave skin cells wherever we go. Therefore, the only possible way to limit government DNA-based surveillance will be to legally constrain governmental collection and use of our DNA.

---

41. In 2002, the National Defense Authorization Act for Fiscal Year 2003 authorized the military to use a database of DNA, collected from service members for the purposes of identifying those killed in combat, for criminal investigations. Pub. L. No. 107-314 §1063, 116 Stat. 2653 (2002).

42. For example, in 2006 the Department of Veterans Affairs lost the names, birth dates, and Social Security numbers of 17.5 million military veterans and personnel. *See* Mary Miller, *Data theft: Top 5 most expensive data breaches*, Christian Science Monitor, May 4, 2011, *available at* http://www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/5.-US-Veterans-Affairs-25-30-million (last visited January 30, 2013).

3. As the Cost of DNA Processing Drops, the Government is Already Taking Steps to Expand Its Collection and Use of DNA

Several judges have warned of the "slippery slope toward ever-expanding warrantless DNA testing." *Pool*, 621 F.3d at 1235 (Schroeder, J., dissenting) (citing *Kincade*, 379 F.3d at 842-71 (Reinhardt, J., dissenting) and 871-75 (Kozinski, J., dissenting)), *opinion vacated* 659 F.3d 761; *see also Mitchell*, 652 F.3d at 429 (Rendell, J., dissenting) ("we may be opening the door to the collection and analysis of DNA for crime-solving purposes from" others with reduced expectations of privacy like students). Those dissents were prescient. Federal, state and local collection, sharing and analysis of DNA profiles and other biometric identifiers have increased significantly over the last several years, and, as Rapid DNA makes DNA processing cheaper, easier and more widely available, it will become possible for even the smallest local police department to create and maintain its own DNA database.

As DNA laws across the country have expanded to cover more crimes and more people, DNA collection has increased dramatically. New samples processed annually through CODIS increased from 1 million in 2007, to approximately 1.3 million in 2008, to nearly 1.7 million samples in 2009, the year Maryland collected Mr. King's DNA.[43] As of December 2012, the National DNA Index

43. *See* Nat'l Inst. of Justice, *DNA Evidence Backlogs: Convicted Offender and Arrestee Samples*, http://www.nij.gov/topics/forensics/lab-operations/evidence-backlogs/convicted-offender-arrestee-samples.htm (last visited January 30, 2013) (noting "This increase is a direct reflection of new state statutes increasing the number of offenses that qualify for collection as well as the trend of collecting samples from arrestees.").

("NDIS," the federal level of CODIS) contained nearly 11.5 million non-forensic profiles.[44] And as a result of arrestee collection laws, states' individual databases are each expanding exponentially as well.[45]

Interest in the potential uses for DNA has also increased. States and the federal government are spending millions of dollars to expand DNA collection capabilities. For example, in 2006, the federal Department of Justice awarded a multi-year, multi-million-dollar contract to Unisys to develop a "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."[46] Since then, the Department of Justice has been rolling out improvements to CODIS that have included enhanced search and analysis capabilities, such as incremental searching, population statistical calculations, efficient processing of large databases up to 50 million

---

44. *See* Fed. Bureau of Investigation, *CODIS—NDIS Statistics*, http://www.fbi.gov/about-us/lab/codis/ndis-statistics (last visited January 30, 2013).

45. *See, e.g.,* Cal. Bureau of Forensic Servs., *DNA Frequently Asked Questions: Effects of the All Adult Arrestee Provision*, http://oag.ca.gov/bfs/prop69/faqs (last visited January 30, 2013) (noting that after California's arrestee DNA collection law was passed in 2009, "the average DNA sample submission rate increased to about 26,500 per month, or about a 120% increase over the average in 2008 of about 12,000 per month).

46. *See* Press Release, *FBI Contracts with Unisys for Development and Deployment of Next-Generation Combined DNA Index System*, Business Wire, October 19, 2006, http://www.businesswire.com/news/home/20061019005514/en/FBI-Contracts-Unisys-Development-Deployment-Next-Generation-Combined (last visited) January 30, 2013).

specimens, and greater interoperability with state and international DNA databases.[47]

This report and the FBI's own website also state that the DOJ will introduce further improvements to CODIS in the near future, including "expanding CODIS capabilities in terms of DNA match technologies (*e.g.*, electropherogram, base composition, full mtDNA sequence, mini-STRs, SNPs)" and kinship searches.[48]

Other branches of the federal government may now collect and process DNA, even from people outside the criminal justice system. Changes to Department of Justice regulations in 2009 require the government to collect DNA "from non-United States persons who are detained under the authority of the United States," whether or not they are implicated in any criminal wrongdoing. 28 C.F.R. §28.12(b). These changes allow agencies like the

---

47. *See* Dep't. of Justice, *Exhibit 300: Capital Asset Summary* 2 (last revised Aug. 1, 2012), *available at* https://my.itdashboard.gov/investment/exhibit300/pdf/011-000002501 (last visited January 30, 2013). For further information on CODIS-related expenditures, *see also* Dep't. of Justice, *Exhibit 300: Capital Asset Plan and Business Case Summary, FBI Combined DNA Index System* 1, February 1, 2010, *available* at http://www.justice.gov/jmd/2011justification/exhibit300/fbi-2011-cjis-wan.pdf (last visited January 30, 2013).

48. *Id.; see also* Fed. Bureau of Investigation, *CODIS—The Future*, *available* at http://www.fbi.gov/about-us/lab/codis/codis_future (last visited January 30, 2013) (noting the re-architecture of CODIS will allow it "to include additional DNA technologies" such as Y-chromosome Short Tandem Repeats (Y-STRs) and mitochondrial DNA, both of which can definitively determine kinship along paternal and maternal lineages, respectively).

Department of Homeland Security ("DHS"), Customs and Border Protection, and Immigration and Customs Enforcement to collect DNA from almost any non-US person they fingerprint, including children as young as 14.[49] DHS itself has estimated that as many as 1 million people who are subject to administrative detention or arrest annually could now be subject to DNA collection.[50]

Other public documents show that U.S. Citizenship and Immigrations Services ("USCIS"), a component of DHS, wants to use Rapid DNA analysis to verify refugee applications and for other purposes.[51] USCIS has stated that DNA should be collected from all immigration applicants—possibly even infants—and stored in the FBI's criminal DNA database.[52] The agency also supports sharing immigrant DNA with "local, state, tribal, international, and other federal partners" including the

---

49. *See* Jennifer Lynch, *DHS Considers Collecting DNA From Kids; DEA and US Marshals Already Do*, Elec. Frontier Found., May 14, 2012, https://www.eff.org/deeplinks/2012/04/dhs-considers-collecting-dna-kids-dea-and-us-marshals-already-do (last visited January 30, 2013) (reporting on and linking to records released through the Freedom of Information Act). DHS has also considered revising its fingerprint rules to allow fingerprint collection from children younger than 14. *Id.* This would, in turn, lower DHS's allowable age for DNA collection.

50. *Id.*

51. *See* Jennifer Lynch, *Rapid DNA: Coming Soon to a Police Department or Immigration Office Near You*, Elec. Frontier Found., Jan. 6, 2013, https://www.eff.org/deeplinks/2012/12/rapid-dna-analysis (last visited January 30, 2013) (reporting on and linking to documents).

52. *Id.*

Department of Defense and Interpol.[53] And these same documents show that the intelligence community and the military are interested in using Rapid DNA to reveal ethnicity, health status, age, and other factors.[54]

Although current federal laws and regulations would need to change before USCIS, DHS and the FBI could rely on DNA processed with Rapid DNA machines,[55] state and local law enforcement agencies across the country could begin using these tools immediately. Rapid DNA manufacturers like IntegenX know this and are encouraging agencies to create their own local DNA databases instead of relying on CODIS.[56] Based on these sales materials, it is not hard to imagine local DNA databases quickly proliferating throughout the 18,000 large and small law enforcement agencies around the country. Given the current state of flux for DNA collection

---

53. *Id.*

54. *Id.* The records are available at https://www.eff.org/file/36189#page/9/mode/1up (last visited January 30, 2013).

55. *See* U.S. Citizenship and Immigration Servs., *SPC Opinions Paper: Expanding DNA Testing in the Immigration Process* 1, *available at* https://www.eff.org/file/36189#page/93/mode/1up (last visited January 30, 2013); Ellen Messmer, *Legal Hurdles Threaten to Slow FBI's 'Rapid DNA' Revolution*, Network World, September 19, 2012 *available at* https://www.networkworld.com/news/2012/091912-fbi-rapid-dna-262596.html (January 30, 2013).

56. *See* IntegenX, *White Paper: The Case for Rapid DNA* (May 2012), *available at* http://integenx.com/wp-content/uploads/2012/05/The-Case-for-Rapid-DNA.pdf (last visited January 30, 2013); John W. Blackledge, *et al.*, *Rapid DNA*, Nat'l Acad. Assoc. Magazine, May-June 2012, at 14.

laws, it is unclear what standards would govern the use and prevent the abuse of these tools. Reducing the cost of DNA processing and making it easy enough for the officer on the street to accomplish with minimal training may mean that law enforcement does not follow the stringent DNA handling procedures currently required by the FBI[57] and that, without oversight, collection procedures could become attenuated from an actual arrest and possibly based on little or no real suspicion of criminal activity.

As shown, the "slippery slope toward ever-expanding warrantless DNA testing" judges throughout the country have predicted is already upon us. *See Pool,* 621 F.3d at 1235 (Schroeder, J., dissenting) (citing *Kincade*, 379 F.3d at 842-71 (Reinhardt, J., dissenting) and 871-75 (Kozinski, J., dissenting)); *see also Mitchell*, 652 F.3d at 429 (Rendell, J., dissenting).

---

57. Even the FBI's procedures have not prevented misconduct in labs. *See* Dan Noyes, *Audit Critical of Santa Clara County Crime Lab*, *ABC Local Station KGO*, October 21, 2012, *available at* http://abclocal.go.com/kgo/story?section=news/iteam&id=8856509 (last visited January 30, 2013) (discussing September 2012 Department of Justice audit of Santa Clara County, California's DNA lab). And as other USCIS public documents note, according to the Department of State, security and chain of custody of DNA samples have had problems in the past. *See* Email from Marcela C. Moglia to Jennifer B. Higgins and Rhonda J. Roberts, July 21, 2009, 2:41 p.m., *available at* https://www.eff.org/file/36189#page/10/mode/1up (last visited January 30, 2013). Even "accredited labs are rife with problems." *See* Senior Policy Council, Options Paper, *Expanding DNA Testing in the Immigration Process*, U.S. Citizenship and Immigration Servs., *available at* https://www.eff.org/file/36189#page/94/mode/1up (last visited January 30, 2013).

CONCLUSION

Warrantless and suspicionless DNA collection from arrestees is the next step toward a future where "all Americans will be at risk . . . of having our DNA samples permanently placed on file in federal cyberspace, and perhaps even worse, of being subjected to various other governmental programs providing for suspicionless searches conducted for law enforcement purposes." *Kincade*, 379 F.3d at 843 (Reinhardt, J., dissenting). This is not merely a "parade of horribles," *Haskell*, 669 F.3d at 1062, but the road we are on. The Maryland Court of Appeals rightly stopped this trajectory. Its decision should be affirmed.

Dated: February 1, 2012

Respectfully submitted,

Jennifer Lynch
Counsel of Record
Lee Tien
Hanni Fakhoury
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, California 94110
(415) 436-9333
jlynch@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation