Case No. 10-15152

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Before the En Banc Panel
(Opinion filed February 23, 2012)

ELIZABETH AIDA HASKELL, REGINALD ENTO, JEFFREY PATRICK LYONS, JR., and AAKASH DESAI, on behalf of themselves and others similarly situated,
Plaintiffs-Appellants,
v.
KAMALA D. HARRIS, Attorney General of California; EVA STEINBERGER, Assistant Bureau Chief for DNA Programs, California Department of Justice,
Defendants-Appellees.

SUPPLEMENTAL BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANTS

On Appeal from the United States District Court
for the Northern District of California
The Honorable Charles R. Breyer
Case No. C 09-04779 CRB

Jennifer Lynch
Hanni Fakhoury
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus curiae Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of amicus.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Statutes

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital age. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. EFF has often served as counsel or amicus in privacy cases, including this case and others considering the constitutionality of DNA testing of pretrial arrestees. *See Maryland v. King,* 133 S.Ct. 1958 (2013); *U.S. v. Pool*, 621 F.3d 1213 (9th Cir. 2010); *U.S. v. Mitchell*, 652 F.3d 387 (3d Cir. 2011); *People v. Buza*, 262 P.3d 854 (Cal. 2011).

Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except undersigned counsel, has authored the brief in whole or in part, or contributed money towards the preparation 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.

California argues in supplemental briefing that mandating DNA collection from people merely arrested for felonies—including non-serious felonies—is constitutional under *Maryland v. King*, 133 S.Ct. 1958 (2013). However, the sharp differences between California and Maryland's statutes, combined with the serious privacy interests implicated by DNA collection, counsel the opposite. Considering that myriad quick and effective identification tools are already at California's disposal—from fingerprints to palm prints to face recognition-capable photographs—this Court should end the expansion of warrantless DNA collection.

ARGUMENT

I. *KING* DID NOT ESTABLISH A *PER SE* RULE AUTHORIZING WARRANTLESS COLLECTION OF DNA DURING BOOKING.

The government argues that *King* established a *per se* rule authorizing the warrantless collection of DNA from all arrestees. Gov.Supp.Br. at 1. It did not; *King* at most upheld such DNA collection for "serious offenses." *King*, 133 S.Ct. at 1978. In rejecting arguments that DNA testing delays undermined their

investigative capacity, *King* noted that "actual release of a *serious offender* as a routine matter takes weeks or months in any event." *Id.* at 1977 (emphasis added). Even Justice Scalia's dissenting opinion recognized this limit, noting that the majority "disguises the vast (and scary) scope of its holding by promising a limitation it cannot deliver": that DNA was only being collected from individuals arrested for "serious offenses." *Id*. at 1989 (Scalia, J., dissenting).

That limited approach is consistent with the command that what is "reasonable" for Fourth Amendment purposes "depends on the context within which a search takes place." *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985). Thus, *per se* exceptions to the Fourth Amendment are disfavored because they often result in "considerable overgeneralization." *See Richards v. Wisconsin*, 520 U.S. 385, 393 (1997) (no blanket exception to Fourth Amendment's "knock and announce" requirement); *Missouri v. McNeely*, 133 S.Ct. 1552, 1561 (2013) (rejecting *per se* rule to permit warrantless blood testing in all drunk driving cases); *id*. at 1564 (noting that "[n]umerous police actions are judged based on fact-intensive, totality of the circumstances analyses rather than according to categorical rules" (citing cases)).

Even when this Court has analyzed DNA testing, it has analyzed the totality of the circumstances presented by the statute at issue. Thus, although this Court upheld Oregon's DNA collection regime in *Rise v. Oregon*, 59 F.3d 1556 (9th Cir.

1995), it did not rely on *Rise* when it reviewed *federal* DNA collection in *U.S. v. Kincade*, 379 F.3d 813 (9th Cir. 2004) (en banc). In fact, apart from noting that *Rise* analyzed DNA collection under the totality of the circumstances test, this Court did not reference *Rise* again. *Kincade*, 379 F.3d at 831-32. Similarly, this Court must analyze California's statutory regime anew instead of presuming *King* is the final word.

II. DNA COLLECTION IMPLICATES SIGNIFICANT PRIVACY INTERESTS.

Personal privacy interests outweigh California's interests in DNA collection. Divided opinions of this court and others have recognized the threat to privacy posed by ever-expanding DNA collection and the need to limit that expansion. *See, e.g., King*, 133 S.Ct. at 1989 (Scalia, J. dissenting); *Haskell v. Harris,* 669 F.3d 1049, 1079 (9th Cir. 2012) (W. Fletcher, J., dissenting); *Kincade*, 379 F.3d at 842 n.3 (Gould, J., concurring) ("the advance of science promises to make stored DNA only more revealing in time"); *id.* 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"); *Mitchell*, 652 F.3d at 424 (Rendell, J., dissenting).

Three aspects of the expanding use of DNA technology must factor into the constitutional analysis of the significance of the difference between California and Maryland's statutes: (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 throughout government and society as a whole, and (3) the very real threats to liberty posed by excessive collection. Taken together, these show that the potential for harm from limitless DNA collection is much greater than any other law enforcement technology previously addressed by the courts.

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

A DNA sample—taken from a simple cheek swab—contains a person's entire genetic makeup. This is private and intensely personal information that 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. *See Kincade*, 379 F.3d at 850 (Reinhardt, J., dissenting) (citation omitted). California retains this genetic data indefinitely. Cal. Penal Code § 299.5(b).[1] California's restrictions to accessing this data cannot cure an otherwise unconstitutional search and seizure. *See U.S. v. Stevens*, 559 U.S. 460, 480 (2010) ("we would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.").

[1] Unlike Maryland, California has no automatic expungement provision. *Compare* Cal. Penal Code § 299(b) (must make written request for expungement) *with* Md. Code. Pub. Safety § 2-511(a) (automatic expungement if no conviction occurs or pardon is granted).

Profiles extracted from DNA samples have their own privacy concerns. For example, California can already infer familial relationships with a high degree of accuracy from profiles and expressly authorizes and conducts such searches.[2] Familial searching disproportionately impacts African Americans because criminal DNA databases contain more DNA from African Americans than other groups in the U.S. population.[3] If familial searching were conducted on a mass scale, as many as 17% of U.S. African Americans could be identified through the DNA profiles already in CODIS (versus only 4% of U.S. Caucasians).[4] This disproportionate representation leads to a "roughly two orders of magnitude higher" rate of false identification.[5] No parallel risk exists for fingerprinting.

Data aggregation—combining CODIS data with other publicly available genetic data—creates additional privacy risks. Currently, tens of thousands of humans have had their genomes completely sequenced, and over a million have

---

[2] *See* FBI, *Familial Searching*, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/familial-searching.

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

[4] *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 2 million profiles in 2006 to 10 million today, so this percentage could now be much higher).

[5] 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.

had high-resolution scans for genetic variants.[6] These numbers are increasing rapidly as the costs of sequencing decline.[7] This means that a substantial and growing fraction of the population has a fourth degree or closer relative whose genetic information is available in public or private databases.

Combining CODIS information with other genetic data 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[8] to specific functional regions within our DNA that influence physical traits or disease predispositions. Access to a profile and information about the profile owner's relatives would, if any near relatives had full genome 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 have recently aggregated data to re-identify anonymized genetic samples—determining not just the name of the person whose sample was present

---

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

[7] *See* JASON (The MITRE Corporation), *The $100 Genome: Implications for the DoD* 2 (Dec. 15, 2010), www.fas.org/irp/agency/dod/jason/hundred.pdf (noting that early attempts to sequence the human genome cost approximately $300 million); Nat'l Human Genome Research Inst., NIH, *Overview of Genetic Testing*, (June 7, 2013) https://www.genome.gov/10002335 (noting that in only "a few years, the sequencing of a patient's entire genome will be an affordable standard diagnostic tool.").

[8] "Linked" in the genetic sense, meaning co-inherited with high probability.

in but also his entire family—showing that "data release, even of a few markers, from one person can spread through deep genealogical ties to identify another person who might have no acquaintance with the person who released his genetic data."[9]

These risks will only increase as more genetic data becomes publicly available.

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

Several judges have rightly warned of the "slippery slope toward ever-expanding warrantless DNA testing." *Pool*, 621 F.3d at 1235 (Schroeder, J., dissenting); *see also King*, 133 S.Ct. at 1989 (Scalia, J., dissenting); *Mitchell*, 652 F.3d at 429 (Rendell, J., dissenting). 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.[10]

[9] Melissa Gymrek, *et al*., *Identifying Personal Genomes by Surname Inference*, 339 Science 321, 322 (January 18, 2013).

[10] 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.

After California began collecting DNA from arrestees, the number of profiles in its state database increased dramatically.[11] A 2010 report noted that California has "one of the most inclusive DNA databases in the country, . . . [comprising] about 3.5% of its population."[12] Due in part to the breadth of its DNA collection laws, California's databank is the largest state database in the country[13] and the third largest in the world.[14] But despite the size of its database, California "is anomalous in the relatively low number of investigations aided."[15]

DNA collection and its attendant risks will continue to increase as local agencies create their own databases[16] and begin to use new "Rapid DNA" technology that can extract a profile in 90 minutes or less. Rapid DNA can be used

---

[11] *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 (noting that after California's arrestee DNA collection law passed, the average DNA submission rate doubled from 12,000 per month in 2008 to 26,500 per month in 2009).

[12] Jeremiah Goulka, *et al.*, RAND, *Toward a Comparison of DNA Profiling and Databases in the United States and England,* 18 (2010), http://www.rand.org/content/dam/rand/pubs/technical_reports/2010/RAND_TR918.pdf ("RAND Report").

[13] *Id.* at 18.

[14] *Brown Announces Elimination of DNA Data Bank Backlog* (Sept. 10, 2007) https://oag.ca.gov/news/press-releases/brown-announces-elimination-dna-data-bank-backlog.

[15] RAND Report at 19.

[16] *See, e.g.,* Goldstein, *supra* note 11 (describing Orange County, California's database).

by non-scientists outside a lab, can process DNA for as little as $100 per sample,[17] and is already used by police in Palm Bay, Florida.[18]

Given the convenience and speed of Rapid DNA, it is likely that officers will soon use it during street-level stops. Rapid DNA results cannot be entered into CODIS,[19] but this may encourage the 500+ law enforcement agencies in California[20] to create local DNA databases. Without hard limits on DNA collection, these tools could easily be used with little or no real suspicion of criminal activity.

C. The Tangible and Intangible Harms of Excessive DNA Collection are Real.

Sloppy policing and systemic DNA lab problems[21] can lead to false identifications that can only occur if the innocent person's profile is already in the

---

[17] *See* Jennifer Lynch, *Rapid DNA: Coming Soon to a Police Department or Immigration Office Near You*, EFF, January 6, 2013, https://www.eff.org/deeplinks/2012/12/rapid-dna-analysis (describing records received through FOIA).

[18] *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.

[19] *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.

[20] Brian A. Reeves, DOJ BJS, *Census of State and Local Law Enforcement Agencies, 2008*, 15 (July 2011) http://www.bjs.gov/content/pub/pdf/csllea08.pdf.

[21] *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 (Sept. 2012); William C. Thompson, *Tarnish on the "Gold Standard:" Understanding Recent Problems in Forensic DNA Testing,* The Champion, Jan./Feb. 2006 at 10-12 (listing

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—even though Anderson had been hospitalized when the murder occurred.[22] In Sacramento, Shawn Ponce was falsely arrested based on his DNA and jailed for five days for two crimes he could not have committed.[23] 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 innocence.[24] Another British citizen was falsely accused of murdering a woman in Italy based solely on DNA.[25] These concrete harms can only occur when innocent persons' DNA is collected and retained. *See King*, 133 S.Ct. at 1989 (Scalia, J., dissenting) (DNA collection "manages to burden uniquely the sole group for whom the Fourth Amendment's protections ought to be most jealously guarded: people who are innocent of the State's accusations.").

---

scandals); http://www.bioforensics.com/articles/Thompson_Champion_Tarnish.pdf.

[22] Henry Lee, *How innocent man's DNA was found at killing scene*, SF Chronicle (June 26, 2013) http://www.sfgate.com/crime/article/How-innocent-man-s-DNA-was-found-at-killing-scene-4624971.php.

[23] *See U.S. 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).

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

[25] Linda Geddes, *DNA super-network increases risk of mix-ups*, New Scientist (Sept. 6, 2011) http://www.newscientist.com/article/mg21128285.500-euro-dna-treaty-risks-false-positives.html.

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. This Court can and should stop this trajectory.

Dated: October 28, 2013

By: */s/ Jennifer Lynch*__

Jennifer Lynch
Hanni M. Fakhoury
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amicus Curiae
Electronic Frontier Foundation

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae In Support Of Plaintiff-Appellant complies with the type-volume limitation of this Court's August 14, 2013 order granting the filing of supplemental amicus brief because this brief contains 2,493 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: October 28, 2013

By: */s/ Jennifer Lynch*__
Jennifer Lynch

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 28, 2013.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, to the following non-CM/ECF participant:

Anne Marie Schubert
Office of the District Attorney
901 G Street
Sacramento, CA 95814-1801

Dated: October 28, 2013

By: */s/ Jennifer Lynch*__
Jennifer Lynch

Counsel for Amicus Curiae
Electronic Frontier Foundation