

Case No. 10-15152
(U.S.D.C. N.D. Cal., Case No. C-09-04779 CRB)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Before the Honorable William A. Fletcher, Milan D. Smith, Jr., Circuit Judges, and
James Dale Todd, Senior District Judge
(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.

**BRIEF AMICUS CURIAE OF ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF REHEARING EN BANC**

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

Hanni M. Fakhoury (SBN 252629)
ELECTRONIC FRONTIER
FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
hanni@eff.org

*Attorney 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

STATEMENT OF INTEREST	1
INTRODUCTION	1
ARGUMENT	3
I. THE WARRANTLESS SEIZURE AND REPEATED SEARCH OF DNA TAKEN FROM MERE ARRESTEES IS UNCONSTITUTIONAL	3
A. The Search at Issue Is A Repeated Intrusion Into A Person’s Sensitive Genetic Information.	4
B. The Totality of the Circumstances Test Cannot Justify the Warrantless and Suspicionless Search of a Mere Arrestee.....	7
C. The Privacy Interests of Individuals Not Stripped of Their Constitutional Rights Outweighs the Government’s Interest in Building Out Its Massive DNA Database.	11
1. Cheaper DNA Analysis Will Lead to More DNA Analysis	12
2. The Government is Already Taking Steps to Expand Its Collection and Use of DNA to Build a Bigger Biometric Database	15
CONCLUSION	18

TABLE OF AUTHORITIES

Cases

<i>Bell v. Wolfish</i> , 441 U.S. 520 (1979)	10
<i>Chandler v. Miller</i> , 520 U.S. 305 (1997)	3
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000)	8, 10, 11
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971)	3
<i>Friedman v. Boucher</i> , 580 F.3d 847 (9th Cir. 2009).....	4, 10
<i>Haskell v. Harris</i> , --- F.3d ---, 2012 WL 589469 (9th Cir. 2012)	<i>passim</i>
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	2
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	2, 5, 11
<i>New Jersey v. T.L.O.</i> , 469 U.S. 325 (1985)	6
<i>Samson v. California</i> , 547 U.S. 843 (2006)	<i>passim</i>
<i>Schmerber v. California</i> , 384 U.S. 757 (1966)	6
<i>Schneckloth v. Bustamonte</i> , 412 U.S. 218 (1973)	3

Treasury Employees v. Von Raab,
489 U.S. 656 (1989) 3, 7

United States v. Brown,
563 F.3d 410 (9th Cir. 2009)..... 3

United States v. Garcia,
474 F.3d 994 (7th Cir. 2007)..... 2

United States v. Jones,
132 S.Ct. 945 (2012) 12, 13

United States v. Kincade,
379 F.3d 813 (9th Cir. 2004) (en banc).....*passim*

United States v. Knights,
534 U.S. 112 (2001) 8, 9, 10, 11

United States v. Miller,
425 U.S. 435 (1976) 13

United States v. Mitchell,
652 F.3d 387 (3d Cir. 2011) (en banc)..... 11

United States v. Pool,
621 F.3d 1213 (9th Cir. 2010),
opinion vacated 659 F.3d 761 (9th Cir. 2011) 2, 5, 15

United States v. Scott,
450 F.3d 863 (9th Cir. 2006)..... 12

Constitutional Provision

U.S. Const. amend. IV*passim*

Other Authorities

California Department of Justice Proposition 69 DNA Data Bank Program
Report for Fourth Quarter 2011 16

Department of Justice, *Exhibit 300: Capital Asset Plan and Business Case Summary, FBI Combined DNA Index System* (2011) 17, 18

FBI, “CODIS—NDIS Statistics” (January 2012) 16

FBI, “CODIS—The Future” 17, 18

Harold J. Kent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 *Tex.L.Rev.* 49 (1995) 7

JASON (The MITRE Corporation), *The \$100 Genome: Implications for the DoD* (Dec. 15, 2010) 14

Jules Epstein, “Genetic Surveillance”—*The Bogeyman Response to Familial DNA Investigations*, 2009 *U. Ill. J.L. Tech. & Pol’y* 141 (2009) 15

Marc Nelson, *Making Sense of DNA Backlogs, 2010—Myths vs. Reality*, National Institute of Justice (Feb. 2011) 15, 16

N. Webster, *An American Dictionary of the English Language* (1828) (reprint 6th ed.1989)..... 5

Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 *Stan L. Rev.* 751 (Apr. 2011) 16

Paul Ohm, *The Fourth Amendment Right to Delete*, 119 *Harv. L. Rev. F.* 10 (2005) 5

Unisys, “FBI Contracts with Unisys for Development and Deployment of Next-Generation Combined DNA Index System” 17

STATEMENT OF INTEREST

The Electronic Frontier Foundation (“EFF”) is a nonprofit, member supported civil liberties organization that 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 served as counsel or amicus in privacy cases, including *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 cases considering the constitutionality of DNA testing of pretrial arrestees. *See United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011); *United States v. Pool*, 621 F.3d 1213 (9th Cir. 2010), *opinion vacated* 659 F.3d 761 (9th Cir. 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. Neither Counsel for appellants or appellees oppose the filing of this brief.

INTRODUCTION

This Court has noted time and again that DNA samples and profiles reveal incredibly sensitive information about individuals. *See Haskell v. Harris*, --F.3d--, 2012 WL 589469, *30 (9th Cir. 2012) (W. Fletcher, J., dissenting) (“Even with

today's technology, however, junk DNA reveals more information than a fingerprint.”); *United States v. Pool*, 621 F.3d 1213, 1216 (9th Cir. 2010), *opinion vacated* 659 F.3d 761 (9th Cir. 2011) (“[r]ecent studies have begun to question the notion that junk DNA does not contain useful genetic programming material.”) (quoting *United States v. Kincade*, 379 F.3d 813, 818 n.6 (9th Cir. 2004) (en banc)); *see also Pool*, 621 F.3d at 1234 (Lucero, J., concurring) (“[t]he DNA profiling system at issue promises enormous potential as an investigatory tool, but its expansion or misuse poses a very real threat to our privacy”). And it is clear “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).

And yet, the panel opinion permitted the government warrantless access to this sensitive information with nothing more than a mere arrest. When examining the government’s intended use of a DNA sample and profile, this Court must confront the “power of technology to shrink the realm of guaranteed privacy.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Courts encountering evolving technologies must reject “mechanical interpretations of the Fourth Amendment.” *Id.* at 35-36. “The meaning of a Fourth Amendment search must change to keep pace with the march of science.” *United States v. Garcia*, 474 F.3d 994, 997 (7th Cir. 2007) (citing *Katz v. United States*, 389 U.S. 347 (1967) and *Kyllo*).

The panel opinion presages a future in which every person's DNA is sampled and profiled. As Judge Kozinski noted in his *Kincade* dissent, “[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.” *Kincade*, 379 F.3d at 872 (Kozinski, J., dissenting). At that point, every person can be “identified” at any place where he or she has been, without suspicion or a warrant.

Accordingly, this Court should grant rehearing en banc.

ARGUMENT

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

Warrantless searches are *per se* unreasonable. See *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973); *United States v. Brown*, 563 F.3d 410, 414-415 (9th Cir. 2009). “[S]earches conducted without grounds for suspicion of particular individuals have been upheld . . . in ‘certain limited circumstances.’” *Chandler v. Miller*, 520 U.S. 305, 308 (1997) (quoting *Treasury Employees v. Von Raab*, 489 U.S. 656, 668 (1989)). Fourth Amendment exceptions are “jealously and carefully drawn” and, therefore, “the burden is on those seeking the exemption to show the need for it.” *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971).

The panel’s Fourth Amendment analysis suffers from three major flaws. It (1) misinterpreted the “intrusiveness” of the actual “search” by looking at its physical aspects; (2) relied on an inapplicable exception to the Fourth Amendment

to justify the search; and (3) ignored the significant and actual privacy interests involved. The en banc court should rehear the panel's decision.

A. The Search at Issue Is A Repeated Intrusion Into A Person's Sensitive Genetic Information.

It is important to be clear about the Fourth Amendment events at issue. The panel viewed DNA collection as a single, extended Fourth Amendment event, including the collection of DNA from an arrestee, laboratory analysis of the DNA sample to generate a profile, placement of the profile into CODIS, and matching of the profile against other DNA profiles stored in CODIS. The panel excluded from its analysis all consideration of the fate and privacy interest of the DNA sample, as well as the interests of an arrestee's family members in their DNA profile and sample.

The better approach is to disaggregate. First, the collection of the DNA sample, as a physical intrusion on the body of the person, is a search and a seizure. *Friedman v. Boucher*, 580 F.3d 847, 852 (9th Cir. 2009). Second, the "ensuing chemical analysis of the sample to obtain physiological data" is also a search. *Skinner*, 489 U.S. at 616.

Third, even if the subsequent placement of the DNA profile into CODIS, running the profile for "hits," and retaining the sample are viewed as "merged" with the DNA analysis, each use of a DNA profile for "matching" is a Fourth Amendment search. *See 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)). To “search” means “[t]o look over or through for the purpose of finding something; to explore.” *Kyllo*, 533 U.S. at 32 n.1 (quoting N. Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed.1989)). Under this common-sense approach, the government engages in a search *each time* it searches CODIS for a match.

It is also clear the continued retention of DNA samples is an indefinite seizure. *See 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.”). This seizure results in an individual’s inability to control the dissemination of 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).

It is also important to remember that unlike a fingerprint, DNA searches involve “intrusion into the widest spectrum of human privacy.” *Pool*, 621 F.3d at 1232 (Lucero, J., concurring); *see also Haskell*, 2012 WL 589469 at *30 (W.

Fletcher, J., dissenting) (“our more recent decisions have explicitly recognized that DNA testing constitutes a greater infringement on privacy than fingerprinting.”). The panel incorrectly measured “intrusion” by reference to physical discomfort, noting DNA collection “is substantially less intrusive, both physically and emotionally, than many of the other types of approved intrusions that are routinely visited upon arrestees.” *Haskell*, 2012 WL 589469 at *9. But “intrusion” is measured by the breadth of the government’s entrance into what was previously a private sphere.

“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). While searching a home for a firearm may not bring the homeowner any physical pain, the search can nonetheless be “intrusive” if it strays beyond what is reasonably necessary to accomplish the purpose of the search. The Fourth Amendment requires this Court to “determine whether the search as actually conducted was 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).

As the breadth of a search expands to enter protected private spaces, the more “intrusive” the search is. Comparing DNA to fingerprints clearly fails to capture the essence of a DNA collection and search. The intrusiveness of a

fingerprint is limited to cataloging the pattern of loops and whorls on a person's finger. DNA, however, can capture a person — and his or her relatives' — medical history, including “genetic defects, predispositions to diseases, and perhaps even sexual orientation.” *Kincade*, 379 F.3d at 850 (Reinhardt, J., dissenting) (quoting Harold J. Kent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 *Tex.L.Rev.* 49, 95-96 (1995) (quotations omitted)); *see also Haskell*, 2012 WL 589469 at *30 (W. Fletcher, J., dissenting). It is far more “intrusive” than a fingerprint, notwithstanding that the physical intrusion in taking a DNA sample is only a buccal swab.

Understanding the real “search” at issue here, it is clear the warrantless search of individuals merely accused of a crime violates the Fourth Amendment.

B. The Totality of the Circumstances Test Cannot Justify the Warrantless and Suspicionless Search of a Mere Arrestee.

The majority's adoption of the “malleable and boundless” totality of the circumstances analysis to the warrantless and suspicionless seizure and repeated search of a pretrial arrestee's DNA was wrong because this analysis simple does not apply here. *Kincade*, 379 F.3d at 860 (Reinhardt, J., dissenting); *see Haskell*, 2012 WL 589469 at *4 (citing *Samson v. California*, 547 U.S. 843, 848 (2006) and *Kriesel*, 508 F.3d at 947-48).

The Fourth Amendment only allows searches unsupported by individualized suspicion in “certain limited circumstances.” *Von Raab*, 489 U.S. at 668. These

exceptions include, “special needs” searches conducted for non-law enforcement purposes. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000). This Court has already found the “special needs” approach cannot be used to justify warrantless DNA collection because it is intended for law enforcement purposes. *See Haskell*, 2012 WL 589469 at *14; *Kriesel*, 508 F.3d at 947; *Kincade*, 379 F.3d at 832.

Another of these “limited circumstances” is probation and parole searches. *See United States v. Knights*, 534 U.S. 112 (2001) (probationers); *Samson*, 547 U.S. at 848 (parolees). In both *Knights* and *Samson*, the Supreme Court upheld a warrantless, non-individualized search “by 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). In both cases, the Court noted that a person’s status as a convicted felon is “salient.” *Samson*, 547 U.S. at 848 (quoting *Knights*, 534 U.S. at 118).

In this Court’s prior cases addressing the constitutionality of the DNA Act, the “totality of the circumstances” applied because “of the well-established principle that parolees and other conditional releasees are not entitled to the full panoply of rights and protections possessed by the general public.” *Kincade*, 379 F.3d at 833; *Kriesel*, 508 F.3d at 946. In both *Kincade* and *Kriesel*, the version of

the DNA collection scheme under review applied only to convicted felons. *Kriesel*, 508 F.3d at 944; *Kincade*, 379 F.3d at 820. As *Kincade* noted, the “transformative changes wrought by a lawful conviction and accompanying term of conditional release are well-recognized” and creates “a severe and fundamental disruption in the relationship between the offender and society.” 379 F.3d at 834-35; *see also Kriesel*, 508 F.3d at 949 (“*Kincade’s* rationale [regarding violent felons] applies with equal force [to nonviolent felons]”).

Here, however, the majority creates a new dividing line by applying this totality of the circumstances test to persons who are mere arrestees. *See Haskell*, 2012 WL 589469 at *8 (“a felony arrestee has a significantly diminished expectation of privacy”). But justifying the search of a mere arrestee by relying on the “totality of the circumstances” test in *Samson* and *Knights* is wrong because a mere arrestee is not the constitutional equivalent of a convicted person.

Samson noted that “[p]robation is ‘one point . . . on a continuum of possible punishments ranging from solitary confinement in a maximum-security facility to a few hours of mandatory community service.’” 547 U.S. at 848 (quoting *Knights*, 534 U.S. at 119). “On 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 850. The Supreme Court ruled that since both probationers and parolees have been *convicted*, a suspicionless search is justified

by the interests of preventing recidivism by convicted felons. *Id.* at 853-54; *Knights*, 534 U.S. at 120-21.

“But pretrial releasees are not probationers” because they “are ordinary people who have been accused of a crime but are presumed innocent.” *Scott*, 450 F.3d at 871-72. And “neither the Supreme Court nor this Court has ever ruled that law enforcement officers may conduct suspicionless searches on pretrial detainees for reasons other than prison security.” *Friedman*, 580 F.3d at 856-57. In both the probation and parole searches upheld in *Knights* and *Samson* and the searches of pretrial detainees in custody recognized in *Bell v. Wolfish*, 441 U.S. 520 (1979), there was a non-law enforcement interest: recidivism and prison security. *See Haskell*, 2012 589469 *29 (W. Fletcher, J., dissenting). But collecting and searching DNA only served the government’s interest in law enforcement investigation.¹

Thus, *Samson* and *Knights* simply do not control this case. Instead, it is controlled by *Edmond*, where the Supreme Court noted it had “never approved a [suspicionless search] whose primary purpose was to detect evidence of ordinary

¹ To the extent the state wants to compare an arrestee to a parolee or probationer because both are under government supervision, it must be remembered that only pretrial release conditions “unquestionably related to the government’s special need to ensure the defendant not abscond” are permitted. *United States v. Scott*, 450 F.3d 863, 872 n. 11 (9th Cir. 2006). It is questionable whether collecting DNA furthers that interest. *See Kriesel*, 508 F.3d at 957 (B. Fletcher, J. dissenting).

criminal wrongdoing” and declined “to approve a program whose primary purpose is ultimately indistinguishable from the general interest in crime control.” *Edmond*, 531 U.S. at 41, 44. Since the search here cannot be justified under the *Samson* and *Knights* totality of the circumstances analysis or *Edmond*’s special needs test, it violates the Fourth Amendment.

C. The Privacy Interests of Individuals Not Stripped of Their Constitutional Rights Outweighs the Government’s Interest in Building Out Its Massive DNA Database.

While the government’s non law-enforcement interests are hardly compelling, the privacy interests at stake are enormous. The panel discounted that relevance partly by characterizing them as future concerns not immediately relevant. *See Haskell*, 2012 WL 589469 at *12 (“we cannot legitimately weigh the constitutionality of the current legal regime by arguing about hypothetical and highly speculative actions that would undeniably violate the DNA Act . . . as now in effect.”). But *Kyllo* explained “the rule [a court] adopts 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 United States v. Mitchell*, 652 F.3d 387, 424 (3d Cir. 2011) (Rendell, J., dissenting) (“we should not be blind to the potential for abuse when assessing the legitimacy of [DNA collection].”). This Court cannot avoid confronting the known implications of a rapidly evolving technology that is being used forensically.

There are two crucial aspects of the increasing deployment of modern DNA technology that this Court must address. First, there is a clear trend toward cheaper DNA analysis. Second, government forensic practices have already greatly expanded their use of DNA technology. Taken together, these facts compel the conclusion that if courts do not insist that Fourth Amendment values be scrupulously observed, the continued evolution of DNA technology will usher in a future where dragnet surveillance by tracking our DNA may be unconstrained.

1. Cheaper DNA Analysis Will Lead to More DNA Analysis

Society has already experienced how new technologies enable things once deemed impossible, to now be done cheaply and efficiently. With surveillance, cheapness and efficiency are not an unalloyed good; while improved surveillance techniques may help law enforcement, they also pose serious privacy risks.

In the past, courts could say that individuals have no reasonable expectation of privacy in public, secure in the fact that surveilling individuals was so costly that it occurred only when the government had a compelling reason to do so. Justice Alito noted recently “[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.” *United States v. Jones*, 132 S.Ct. 945, 963 (2012) (Alito, J., concurring in the judgment). But as *Jones* itself demonstrated, today’s technology

has made it easier to use GPS and cell phone tracking to make such surveillance routine. *See Jones*, 132 S.Ct. at 948 (finding 28 day continuous GPS surveillance of car violates Fourth Amendment).

Traditionally, individuals have no reasonable expectation of privacy in records of their transactions held by business. *See United States v. Miller*, 425 U.S. 435 (1976). Today, this idea is being called into question as our lives are thoroughly documented in myriad transactions, and virtually everything we do electronically is recorded somewhere. *See Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring) (“it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”). But the conclusion is inescapable: cost matters to privacy and to Fourth Amendment values.

This matters because society faces the same set of issues for DNA technology. Ten years ago, the cost of analyzing DNA was too great to not pose a risk to ordinary Americans. Today, it is much cheaper; a recent report prepared for the U.S. Department of Defense predicts the cost to sequence an entire human genome could drop to \$100 by 2013. JASON (The MITRE Corporation), *The*

\$100 Genome: Implications for the DoD, at 11 (Dec. 15, 2010) (hereinafter “JASON Report”).²

The JASON report explains that while the first draft sequences of the human genome cost about \$300 million, improvements in “second-generation” DNA sequencing platforms in the past five years have reduced costs such that “[a]n entire human genome can now be sequenced in a matter of days for a retail cost of \$20,000,” and “third-generation”³ sequencing technology will mean that “DNA sequencing costs will no longer be a factor limiting personal human genomics technologies.” *Id.* at 2. Indeed, the cost “will likely fall to less than \$1000 by 2012, and to \$100 by 2013.” *Id.* at 12.

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. If, as some argue, we have no privacy interest in our

² Available at www.fas.org/irp/agency/dod/jason/hundred.pdf (last visited March 16, 2012).

³ The JASON report explains “new technologies, called third-generation sequencing systems,” are expected to account for this cost reduction. JASON Report at 16. One company, Ion Torrent, has developed advanced DNA sequencing chips that reduce costs even though they are made with “chip fabrication facilities constructed in 1995;” “[d]ramatic” improvements “can be achieved simply by using more recent chip fabrication facilities . . . [and] [t]herefore, DNA sequencing chips that permit complete collection of a human genome for less than \$100 seems within easy reach.” *Id.* at 17-18.

“abandoned” DNA, *see* Jules Epstein, “*Genetic Surveillance*”—*The Bogeyman Response to Familial DNA Investigations*, 2009 U. Ill. J.L. Tech. & Pol’y 141, 151 (2009), then there will be no legal constraint on government collection of our DNA from public places. The only possible way to limit government DNA-based surveillance will be to legally constrain governmental use of our DNA.

2. The Government is Already Taking Steps to Expand Its Collection and Use of DNA to Build a Bigger Biometric Database

One judge has 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. Those dissents were prescient. The government’s collection, sharing and analysis of DNA profiles and other biometric identifiers has significantly increased over the last several years.

As a result of the expansion of state and federal DNA collection statutes, collection for law enforcement and law enforcement-related purposes has amplified. In 2009 alone, nearly 1.7 million samples from convicted offenders and arrestees were processed through CODIS. *See* Marc Nelson, *Making Sense of DNA Backlogs, 2010—Myths vs. Reality*, National Institute of Justice, 7–8 (Feb. 2011).⁴ As of January 2012, the National DNA Index (“NDIS,” the federal

⁴ Available at <http://www.ncjrs.gov/pdffiles1/nij/232197.pdf> (last visited March 16, 2012).

level of CODIS) contains over 10,484,400 offender profiles, and states' individual databases are each expanding as well. *See* FBI, "CODIS—NDIS Statistics," (January 2012).⁵

Current federal technology cannot meet the demands of these expanded collection programs. A Department of Justice ("DOJ") sponsored report noted the "year-end backlog of offender samples has increased steadily, from 657,166 in 2007, to 793,852 in 2008, to 952,393 in 2009." Nelson, *Making Sense of DNA Backlogs* at 8. Current DNA technology cannot efficiently and accurately conduct the kinds of analyses, such as familial or partial searching, that the government wants conducted on DNA it has already collected. *See* Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 *Stan L. Rev.* 751, 764-65 (Apr. 2011) (noting the current version of CODIS "is poorly designed for identifying true leads where partial matches are uncovered").

To meet these demands, the DOJ has spent the last six years attempting to "re-architect the CODIS software" to expand its capabilities. *See* FBI, "CODIS—

⁵ *Available at* <http://www.fbi.gov/about-us/lab/codis/ndis-statistics> (last visited March 16, 2012). California added 30,409 profiles to its state-level database between October 1 and December 31, 2011. *See* California Department of Justice Proposition 69 DNA Data Bank Program Report for Fourth Quarter 2011, *available at* [http://oag.ca.gov/sites/all/files/pdfs/bfs/quarterlyrpt.pdf?](http://oag.ca.gov/sites/all/files/pdfs/bfs/quarterlyrpt.pdf) (last visited March 16, 2012). California has 1,930,306 DNA profiles in its database. *Id.*

The Future.”⁶ In 2006, the DOJ 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.” See Unisys, “FBI Contracts with Unisys for Development and Deployment of Next-Generation Combined DNA Index System.”⁷ The DOJ has stated it plans to roll out a new version of CODIS sometime in 2012. See Department of Justice, *Exhibit 300: Capital Asset Plan and Business Case Summary, FBI Combined DNA Index System*, 1 (2011).⁸ This latest version will include improvements in search and analysis capabilities, including incremental searching, population statistical calculations, efficient processing of large databases up to 50 million specimens, and partial profile indicators, or familial searches. *Id.* It will also allow greater interoperability with state and international DNA databases. *Id.*

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

⁶ Available at http://www.fbi.gov/about-us/lab/codis/codis_future (last visited March 16, 2012).

⁷ Available at https://www.unisys.com/products/news_a_events/all_news/10198717.htm (last visited March 16, 2012).

⁸ Available at <http://www.justice.gov/jmd/2011justification/exhibit300/fbi-2011-cjis-wan.pdf> (last visited March 16, 2012).

composition, full mtDNA sequence, mini-STRs, SNPs)” and kinship searches. *Id.*; *see also* FBI, “CODIS—The Future,”⁹ (noting the re-architecture of CODIS will allow it “to include additional DNA technologies).”

As shown above, the “slippery slope toward ever-expanding warrantless DNA testing” dissenting judges have predicted, is already upon us. *See Kincade*, 379 F.3d at 842-71 (Reinhardt, J., dissenting).

CONCLUSION

The panel’s acceptance of warrantless and suspicionless DNA collection from all arrestees is the next step towards 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 horrors,” *Haskell*, 2012 WL 589469 at *12, but the road we are presently on. “The time to put the cork back in the brass bottle is now—before the genie escapes.” *Id.* at 875 (Kozinski, J., dissenting). The petition for rehearing en banc should be granted.

⁹ *Available* at http://www.fbi.gov/about-us/lab/codis/codis_future (last visited March 16, 2012).

Dated: March 19, 2012

Respectfully submitted,

/s/ Hanni M. Fakhoury
HANNI M. FAKHOURY
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
hanni@eff.org

*Attorneys 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 Rehearing En Banc complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) and 9th Cir. R. 29-2(c)(2) because this brief contains 4,157 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: March 19, 2012

Respectfully submitted,

/s/ Hanni M. Fakhoury
HANNI M. FAKHOURY
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
hanni@eff.org

*Attorneys 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 March 19, 2012.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: March 19, 2012

Respectfully submitted,

/s/ Hanni M. Fakhoury
HANNI M. FAKHOURY
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
hanni@eff.org

*Attorneys for Amicus Curiae
Electronic Frontier Foundation*