NO. 09-10303

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

JERRY ARBERT POOL,

DEFENDANT-APPELLANT.

On Appeal From The United States District Court
For The Eastern District of California
Case No. 2:09-cr-00015 EJG-1
Honorable Edward J. Garcia, Senior District Judge

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, CENTER FOR CONSTITUTIONAL RIGHTS, NATIONAL IMMIGRATION PROJECT OF THE NATIONAL LAWYER'S GUILD AND GENERATIONS AHEAD IN SUPPORT OF DEFENDANT/APPELLANT AND REVERSAL

Hanni Fakhoury (SBN 252629)
Lee Tien (SBN 148216)
Jennifer Lynch (SBN 240701)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org
Attorneys for Amici Curiae

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, Amici Curiae Electronic Frontier Foundation, Center for Constitutional Rights, National Immigration Project of the National Lawyers Guild, and Generations Ahead (collectively, "Amici") state that none of Amici has a parent corporation, and that no publicly held corporation owns 10% or more of the stock of any of Amici.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTE

STATE STATUTE

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

STATEMENT OF INTEREST

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 *National Aeronautics and Space Administration v. Nelson*, 131 S.Ct. 746 (2011), and *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

The Center for Constitutional Rights ("CCR") is a national non-profit legal, educational, and advocacy organization dedicated to advancing and protecting the rights guaranteed by the United States Constitution and the Universal Declaration of Human Rights. CCR has advocated and litigated around important Fourth Amendment issues for decades, and currently represents New Yorkers who have been unlawfully stopped and frisked by the NYPD in *Floyd v. City of New York* No. 08civ01034 (S.D.N.Y 2008); immigration advocates seeking information regarding Secure Communities, Next Generation Identification, and other federal programs in *National Day Laborer Organizing Network v. U.S. Immigration and Customs Enforcement Agency,* 10Civ2705 (S.D.N.Y. 2010) and current and former

prisoners and detainees suing over mistreatment in *Turkmen v. Ashcroft,* No. 02cv2307 (E.D.N.Y 2002) and *Aref v. Holder*, No. 10-0539 (D.D.C. 2010).

The National Immigration Project of the National Lawyers Guild is a non-profit membership organization of immigration attorneys, legal workers, grassroots advocates, and others working to defend immigrants' rights and to secure a fair administration of the immigration and nationality laws. We have a direct interest in ensuring that immigration enforcement actions and custody decisions involving immigrants comply with the Constitution.

Generations Ahead is a non-profit, public policy organization that works to ensure that public uses of human genetic information and technology are fair and equitable. As an organization committed to racial equity, we have an interest in ensuring that the collection and use of DNA in the criminal justice system is constitutional and just. We expand the public debate and promote policies on genetic technologies that protect human rights and affirm our shared humanity. We seek to ensure inclusion, fairness and equality for all people in the use of genetic technologies now, and for generations ahead.

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

Neither Counsel for Appellant Jerry Pool nor Appellee the United States of America oppose the filing of this brief.

I. INTRODUCTION

In this case, the government defends the warrantless, suspicionless search and seizure of a person's most private and personal information—his DNA. The government bears a heavy burden to show the collection and unending retention of DNA from a person merely arrested for a crime falls into one of the limited exceptions to the Fourth Amendment's warrant requirement. The government has not met its burden.

This Court has already acknowledged that "DNA stores and reveals massive amounts of personal, private data about that individual," including "the person's health, their propensity for particular disease, their race and gender characteristics, and perhaps even their propensity for certain conduct." *United States v. Kriesel*, 508 F.3d 941, 948 (9th Cir. 2007) (quoting *United States v. Kincade*, 379 F.3d 813, 842 n.3 (9th Cir. 2004) (en banc) (Gould, J., concurring)). Even the panel recognized that DNA samples and profiles reveal sensitive information about individuals. *United States v. Pool*, 621 F.3d 1213, 1216 (9th Cir. 2010) ("[r]ecent studies have begun to question the notion that junk DNA does not contain useful genetic programming material.") (quoting *Kincade*, 379 F.3d at 818 n.6); *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*, at 842 n.3 (Gould, J., concurring).

When examining the government's intended use of Mr. Pool's 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). The Supreme Court made clear in *Kyllo* that courts encountering evolving technologies must reject "mechanical interpretations of the Fourth Amendment." *Id*. at 35-36. Yet the government's attempt to analogize DNA profiles to traditional fingerprints by labeling both "identification" exemplifies a "mechanical" Fourth Amendment interpretation that loses sight of the fact DNA not only reveals far more about a person than a fingerprint, but is also "identification" for the sole purposes of law enforcement "investigation."

Instead, when conducting the Fourth Amendment analysis of the warrantless search and seizure here, this Court must acknowledge the current and future backdrop behind this search:

- The government must collect DNA samples to create DNA profiles, so any claim that the government's search and seizure does not implicate Mr. Pool's most private bodily information is false.
- The government retains both DNA profiles and samples almost indefinitely.

- The government uses once-collected DNA profiles and samples repeatedly for purposes unrelated to any one defendant's identity. *See* Appellee's Brief at 32, Response of the United States to the Petition for Rehearing En Banc at 16.
- The government has, and will continue to steadily 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.

The Fourth Amendment was a response to "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*, --- U.S. ---, 131 S.Ct. 2074, 2084 (2011). The panel opinion, however, 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 reverse the panel opinion.

II. 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 four major flaws. It (1) misinterpreted the "intrusiveness" of the actual "search" by looking at its physical aspects; (2) incorrectly shifted the burden onto Mr. Pool, rather than require the government to prove the DNA Act's constitutionality; (3) relied on a inapplicable exception to the Fourth Amendment to justify the search; and (4) ignored the significant and actual privacy interests involved. This court should reverse its 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 buccal swab collection of the DNA sample from Mr. Pool, laboratory analysis of the sample to generate a DNA profile according to CODIS specifications, placement of the profile into CODIS, and matching of Mr. Pool's profile against other DNA profiles stored in CODIS. The panel excluded from its analysis all consideration of the fate of Mr. Pool's DNA sample, and thus his privacy interest in his DNA sample. It also excluded the interests of Mr. Pool's family members in both his 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. *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 616 (1989) (blood draw, urine test); *Friedman v. Boucher*, 580 F.3d 847, 852 (9th Cir. 2009) (buccal swab). 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 DNA profile for CODIS "hits," and retaining Mr. Pool's DNA sample are viewed as "merged" with the DNA analysis, each use of DNA profiles for "matching" is a Fourth Amendment search. *See Kriesel*, 508 F.3d at 956 (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). The panel incorrectly measured "intrusion" by

reference to physical discomfort, noting DNA collection "is 'minimally invasive both in terms of the bodily intrusion it occasions, and the information it lawfully produces.'" *Pool*, 621 F.3d at 1222 (quoting *Kincade*, 397 F.3d at 838). But "intrusion" should instead be 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. As noted by the Supreme Court, 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)). 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 Panel Incorrectly Shifted the Burden Onto Mr. Pool.

This Court has made clear "that the *government* bears a heavy burden of demonstrating that exceptional circumstances justified a departure from the normal procedure of obtaining a warrant." *United States v. Driver*, 776 F.2d 807, 810 (9th Cir. 1985) (citations and quotations omitted) (emphasis added).

The panel, however, flipped this on its head. Instead of requiring the government to prove "exceptional circumstances" justifying the warrantless collection of Mr. Pool's DNA, it found he "*has not shown* that (1) the government could, at this time, actually use the DNA information for arguable improper purposes, (2) the government could do so without further legislation,[1] or (3) the

[1] "Although a CODIS profile contains less information than a DNA sample by several orders of magnitude, law enforcement must, of course, collect a DNA sample to create a DNA profile." *Pool*, 621 F.3d at 1231 (Lucero, J., concurring). So current legislation authorizes seizure of far more genetic information than "junk DNA."

government has any intent to use the information." *Pool*, 621 F.3d at 1223 (emphasis added).

To the extent the majority upheld the DNA Act because Mr. Pool failed to demonstrate it was unconstitutional, the panel "misallocate[d] the burden of proof." *Pool*, 621 F.3d at 1237 (Schroeder, J., dissenting). Applying the correct burden, it is clear the government cannot prove its interests outweigh the significant privacy interests implicated by collecting DNA from mere arrestees.

C. No Exception to the Fourth Amendment's Warrant Requirement Can Justify the Search.

1. Because DNA Collection Only Furthers Law Enforcement Interests, the Special Needs Test Does Not Justify the Search.

Suspicionless, warrantless searches have been upheld in limited circumstances when "designed to serve 'special needs, beyond the normal need for law enforcement.'" *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000) (quoting *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)).

This Court has already found the "special needs" approach cannot be used to justify warrantless DNA collection. *See Kriesel*, 508 F.3d at 947; *Kincade*, 379 F.3d at 832. This is because CODIS is maintained for law enforcement purposes, including running an arrestee's DNA against DNA obtained from other crime scenes for the purpose of solving unrelated crimes. The panel acknowledges this

reality, noting the "government's interests in DNA samples for law enforcement purposes are well established." *Pool*, 621 F.3d at 1222.

The government's amici only highlight that DNA collection serves no purpose but to assist law enforcement. DNA Saves writes in its brief "DNA identification of arrestees is a crucial law enforcement tool," and "the government has a compelling interest in solving and preventing crimes, and DNA identification serves it by making criminal investigations more effective and efficient." Brief for Amicus Curiae DNA Saves at 2, 18. The State of California provides examples of "how collecting DNA samples at the time of arrest assist law enforcement in solving crimes that may not have been solved." Brief of Amicus Curiae State of California at 24.[2]

Yet, despite these broad and unsupported claims that collecting DNA from arrestees will improve crime control, the government and its amici also argue that the warrantless and suspicionless search and seizure of Mr. Pool's DNA is necessary for "identification." *See Pool*, 621 F.3d at 1220 ("The government, however, asserts that it only seeks to determine Pool's identification."); Brief for Amicus Curiae DNA Saves at 7 ("Pool's DNA sample would be used solely for

[2] Despite the State of California's claims that collecting DNA from arrestees helps solve crime, *see* Brief of Amicus Curiae State of California at 23-24, it cites no studies or statistics showing DNA collection from arrestees leads to convictions that would not have otherwise occurred without the DNA. This is one example of how the government failed to meet its burden.

identification purposes."); Brief of Amicus Curiae State of California at 20 ("the sole purpose of collecting DNA is to identify"). The panel notes "the government seeks only [Pool's] definitive identification which it relates to its ability to check on his activities while on pre-trial release." *Pool*, 621 F.3d at 1225. This distorts the word "identification" beyond recognition.

No one questions the government needed to confirm Mr. Pool was the actual person named in the indictment. That fact, however, was satisfied by traditional procedures, including fingerprinting. What the government and its amici call a compelling interest in "identification" is something more than just making sure the correct person was arrested: it is primarily an interest in entering Mr. Pool's DNA profile into the CODIS database, looking for matches between his DNA profile and other DNA profiles in CODIS, and retaining his DNA profile and sample for future searches. In other words, the government uses CODIS to "identify" other crimes and crime scenes Mr. Pool may be connected to.[3]

This interest in forensic identification of DNA left at a crime scene is just another word for law enforcement. It is clearly not an interest in confirming an arrestee's identity. Nor could it be since the FBI explicitly explains CODIS access

[3] "Identify" has two definitions: (1) "[t]o prove the identity of (a person or thing)" and, (2) "[t]o look upon as being associated (with). *Black's Law Dictionary*, (9th ed. 2009). The government and its amicus hope to lure the Court into believing the DNA Act does the former, when in practice the government uses Mr. Pool's DNA for the latter.

is given "to criminal justice agencies for law enforcement identification purposes." "Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System."[4] Further, the well-documented backlog in processing DNA actually makes it a poor method of "identifying" an arrestee as the correct defendant, since months can elapse before a sample is actually tested.[5] And to the extent the government wants Mr. Pool's DNA to supervise him while on bail, "the fact that a DNA entry is permanently lodged in CODIS at the very least detracts from the weight afforded the government's claim that the statute is truly designed as a supervisory tool." *Kriesel*, 508 F.3d at 957 (B. Fletcher, J., dissenting).[6] Thus, the two definitions of "identification" should not be conflated.

Because the DNA Act is solely concerned with furthering law enforcement purposes, it cannot be justified under the special needs exception to the Fourth Amendment. *See United States v. Scott*, 450 F.3d 863, 872 (9th Cir. 2006) (special needs doctrine did not justify suspicionless drug testing of pretrial releasee).

---

[4] *Available at* http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet (last visited July 20, 2011).

[5] As of 2009, there was a national backlog of almost 1 million samples. *See* Marc Nelson, *Making Sense of DNA Backlogs, 2010—Myths vs. Reality*, National Institute of Justice, 8 (Feb. 2011), *available at* http://www.ncjrs.gov/pdffiles1/nij/232197.pdf (last visited July 23, 2011).

[6] *Kriesel* involved a defendant who violated his supervised release by repeatedly testing positive for drugs. Judge Fletcher noted "[i]ronically, the authorities had all the tools they needed to detect the recidivism without resort to DNA." *Kriesel*, 508 F.3d at 957 (B. Fletcher, J., dissenting).

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

The bigger problem with the majority's Fourth Amendment analysis is its 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. *Kincade*, 379 F.3d at 860 (Reinhardt, J., dissenting). This analysis simply does not apply here.

The Fourth Amendment only allows searches unsupported by individualized suspicion in "certain limited circumstances." *Von Raab*, 489 U.S. at 668. These exceptions include, as explained above, "special needs" searches conducted for non-law enforcement purposes. *See Edmond*, 531 U.S. at 37. Another of these "limited circumstances" are probation and parole searches. *See United States v. Knights*, 534 U.S. 112 (2001) (probationers); *Samson v. California*, 547 U.S. 843 (2006) (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 was "salient." *Samson*, 547 U.S. at 848 (quoting *Knights*, 534 U.S. at 118).

In this Court's two prior cases addressing the constitutionality of the DNA Act, the "totality of the circumstances" was applied because there was "some legitimate reason for the individual having less than the full rights of a citizen." *Pool*, 621 F.3d at 1219 (citing *Kincade*, 379 F.3d at 833); *see also Kriesel*, 508 F.3d at 946. In both *Kincade* and *Kriesel*, the version of the DNA Act 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 panel invents a new dividing line when it declares a "finding of probable cause [i]s a 'watershed event' that allows for the totality of the circumstances exception to the Fourth Amendment's warrant requirement." *Pool*, 621 F.3d at 1228. Justifying the search of a mere arrestee by relying on *Samson* and *Knights* is wrong because, as stated by Judge Schroeder in her dissent, "[i]f there was . . . a 'watershed event' that justified what would otherwise be an

unconstitutional seizure, the event was a conviction; not a post-arrest probable cause determination." *Pool*, 621 F.3d at 1236 (Schroeder, J., dissenting).[7]

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),

[7] Ignoring the distinction between individuals convicted of a felony and those merely arrested would essentially eliminate the need for jury trials. For if an arrest is enough to trigger the same deprivation of constitutional rights as a conviction, the presumption of innocence is meaningless.

there was a non-law enforcement interest: recidivism and prison security. Here, as described earlier, the only interest in collecting and searching DNA is for law enforcement purposes.[8]

Thus, *Samson* and *Knights* simply do not control this case. Instead, it is controlled by *Edmond*, which noted the Supreme Court had "never approved a [suspicionless search] whose primary purpose was to detect evidence of ordinary 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. The search here therefore cannot be justified under the *Samson* and *Knights* totality of the circumstances analysis.

[8] To the extent the government compares Mr. Pool 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. *Scott*, 450 F.3d at 872 n.11. It is questionable whether collecting DNA furthers that interest. *See Kriesel*, 508 F.3d at 957 (B. Fletcher, J. dissenting). At a minimum, the government has again failed to carry its burden in demonstrating DNA collection is necessary to supervise pretrial releases, particularly in light of the testing backlog. *See supra,* notes 5 and 6, above. The government, in another example of not carrying its burden, has not provided one actual example – let alone studies or statistics – of how DNA collection assists with preventing defendants from absconding.

D. 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 for arrestees and society as a whole are enormous.

1. Current Government Practices Create a Substantial Risk of Dragnet Surveillance Given the Growth of DNA Collection and the Trend Toward Cheaper DNA Analysis.

Members of this Court have already recognized that DNA analysis 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. The panel, while not entirely ignoring these concerns, discounted their relevance partly by characterizing them as future concerns not immediately presented to this case. *Kyllo*, however, stands for the proposition that courts cannot avoid confronting the known implications of a rapidly evolving technology that is being used forensically.

There are three 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. Third, non-forensic practices have also greatly expanded the scope of DNA collection. Taken together, these facts

militate toward 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.

a. As the Cost of DNA Analysis Continues to Decline, It Will Become Faster, Easier and Much More Common to Conduct Even More Intrusive DNA Searches.

Society has experienced how new technologies enable it to do things it could not do before and to do those things more cheaply and efficiently. But where surveillance is concerned, cheapness and efficiency are not an unalloyed good; improved surveillance techniques may well aid law enforcement in criminal investigation, but they also pose risks to our privacy.

In the past, the Supreme Court 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. *See e.g., United States v. Knotts*, 460 U.S. 276, 281-82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."). Today, technology has made it so much easier to use GPS tracking, cellphone tracking, or audio and video surveillance in public places, that surveillance is now routine. *See e.g., United States v. Pineda–Moreno*,

591 F.3d 1212 (9th Cir. 2010) (warrantless GPS surveillance of car does not violate Fourth Amendment).

Similarly, in the past, the Supreme Court said 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, our lives are thoroughly documented in myriad transactions and virtually everything we do electronically is recorded somewhere. Cost therefore matters to privacy and to Fourth Amendment values.

This is relevant because society faces the same set of issues for DNA technology. Even ten years ago, the cost of analyzing DNA was so great it did not pose a risk to ordinary Americans. Today, DNA analysis 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").[9]

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

[9] *Available at* www.fas.org/irp/agency/dod/jason/hundred.pdf (last visited July 23, 2011).

$20,000," and "third-generation"[10] DNA 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 need to think about the privacy expectation in our 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 "abandoned" DNA, *see* Brief for Amicus Curiae DNA Saves at 30 (citing 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.

[10] The JASON report explains "new technologies, called third-generation sequencing systems," are expected to account for this cost reduction. JASON Report at 16. Technology being developed by Pacific Biosciences "should reduce reagent costs, increase read lengths, and dramatically reduce the time needed to sequence each nucleotide." *Id*. Another 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.

b. The Government Has Greatly Expanded Its Collection and Use of DNA and Other Biometrics Identifiers and Has Plans to Build Even More Powerful Biometrics Collection and Analysis Tools.

In her dissent, Judge Schroder recalled the *Kincade* dissenters' warning of a "slippery slope toward ever-expanding warrantless DNA testing." *Pool*, 621 F.3d at 1235 (Schroder, J., dissenting) (citing *Kincade*, 379 F.3d at 842-71 (Reinhardt, J., dissenting) and 871-75 (Kozinski, J., dissenting)). Those dissents were prescient. In the seven years since *Kincade*, the government's collection, sharing and analysis of DNA profiles and other biometric identifiers has expanded significantly.

As a result of the expansion of the DNA Act and state DNA collection statutes, DNA collection for law enforcement and law enforcement-related purposes has increased exponentially. 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).[11] As of 2011, the National DNA Index ("NDIS," the federal level of CODIS) contains over 9,748,870 offender profiles,

[11] *Available at* http://www.ncjrs.gov/pdffiles1/nij/232197.pdf (last visited July 23, 2011).

and states' individual databases are each expanding as well. *See* FBI, "CODIS—NDIS Statistics," (June 2011).[12]

Some have predicted even greater federal accumulation of DNA samples once the Department of Homeland Security ("DHS") fully implements its program to collect samples from "non-United States persons who are detained under the authority of the United States" under 42 U.S.C. § 14135a(a)(1)(A).[13] As DHS may detain "non-United States persons" for purely civil rather than law enforcement purposes, such as overstaying a visa, this could result in expanding CODIS to contain hundreds of thousands of profiles of people who have never interacted with the criminal system. *See Padilla v. Kentucky*, --- U.S. ---, 130 S.Ct. 1473, 1481 (2010) ("deportation is a particularly severe 'penalty,' . . . but it is not, in a strict sense, a criminal sanction . . . removal proceedings are civil in nature") (citations omitted).

---

[12] *Available at* http://www.fbi.gov/about-us/lab/codis/ndis-statistics (last visited July 23, 2011). California added 56,969 profiles to its state-level database between October 1 and December 31, 2010. *See* California Department of Justice Proposition 69 DNA Data Bank Program Report for Fourth Quarter 2010, *available* at http://ag.ca.gov/bfs/pdf/quarterlyrpt.pdf (last visited July 23, 2011). California has 1,748,480 DNA profiles in its database. *Id.*

[13] *See e.g.*, Julia Preston, "Immigrants' DNA to flood U.S. database," *International Herald Tribune*, Feb. 5, 2007 (quoting Justice Department officials as saying "the goal . . . is to make DNA sampling as routine as fingerprinting for anyone detained by federal agents" and noting in 2006, "federal customs, Border Patrol and immigration agents detained more than 1.2 million immigrants."). *Available at* https://www.nytimes.com/2007/02/05/world/americas/05iht-dna.4481568.html (last visited July 23, 2011).

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 federal DNA technology also 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 five years attempting to "re-architect the CODIS software" to expand its capabilities. *See* FBI, "CODIS—The Future."[14] 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 that will greatly accelerate the DNA matching process." *See* Unisys, "FBI Contracts with Unisys for Development and Deployment of Next-Generation

[14] *Available* at http://www.fbi.gov/about-us/lab/codis/codis_future (last visited July 23, 2011).

Combined DNA Index System."[15] While the current status of Next Generation CODIS is unclear,[16] the DOJ has stated it plans to roll out a new version of CODIS sometime in 2011-2012. *See* Department of Justice, *Exhibit 300: Capital Asset Plan and Business Case Summary, FBI Combined DNA Index System*, 1 (2011).[17] 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

[15] *Available at* https://www.unisys.com/products/%20news_a_events/all_news/10198717.htm (last visited July 23, 2011).

[16] Contrast this with the FBI's other "Next Generation" biometric database, called "Next Generation Identification" or "NGI," which promises to "offer state-of-the-art biometric identification services," including "advanced fingerprint identification technology" and "multimodal" identification that includes iris scans, palm prints, and voice and facial recognition technology. *See* FBI, "Next Generation Identification" *available at* http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited July 23, 2011). In fact, the FBI is already building out the NGI database with fingerprints from the DOJ's Integrated Automated Fingerprint Identification System ("IAFIS") as well as the Department of Homeland Security's IDENT and the Department of State's US-VISIT fingerprint collection programs. *See* Center for Constitutional Rights, *New Documents Reveal Behind-the-Scenes FBI Role in Controversial Secure Communities Deportation Program*," (July 6, 2011) at http://ccrjustice.org/newsroom/press-releases/new-documents-reveal-behind-scenes-fbi-role-controversial-secure-communities-deportation-program (last visited July 23, 2011).

[17] *Available* at www.itdashboard.gov/?q=investment/exhibit300/pdf/011-10-01-03-01-2501-00 (last visited July 23, 2011).

future, including "expanding CODIS capabilities in terms of DNA match technologies (*e.g.* electropheragram, base composition, full mtDNA sequence, mini-STRs, SNPs)" and kinship searches. *Id.; see also* FBI, "CODIS—The Future,"[18] (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" the *Kincade* dissenters predicted is already upon us. 379 F.3d at 842-71 (Reinhardt, J., dissenting).

c. DNA Collection Has Expanded In Non-forensic Contexts As Well.

The massive amount of DNA collection and analysis occurring in the law enforcement context may be matched by DNA collection in other areas of society, from military DNA collection,[19] to personal DNA testing,[20] to blood and tissue

[18] *Available* at http://www.fbi.gov/about-us/lab/codis/codis_future (last visited July 23, 2011).

[19] The JASON report recommended the Department of Defense collect and archive DNA samples from all military personnel now and "[p]lan for the eventual collection of complete human genome sequence data." JASON Report at 50. This year, the Army issued a solicitation suggesting it may plan to follow JASON's recommendations. *See* U.S. Army, *Archive of Samples for Long-term Preservation of RNA and Other Nucleic Acids*, Small Business Innovation Research Program, A11-107 (2011) *available at* http://www.dodsbir.net/sitis/display_topic.asp?Bookmark=%40675 (last visited July 23, 2011).

[20] Last year, several drugstores planned to sell at-home personal genetic testing kits that required purchasers to send a saliva sample to the manufacturer, Pathway Genomics, who would analyze the sample and post results online. *See* Sandra Jones, "Genetic test kits to hit stores amid controversy," *Chicago Tribune* May 11,

samples collected for public health purposes. While some rules have been set up to regulate collection and sharing of these DNA samples, the edges are hazy. And it has been shown in sensitive data collection contexts outside of DNA[21] that there is a high risk these treasure troves of data will be compromised or used for purposes beyond their original intention.

Newborn blood sample collection exemplifies these risks. Although the *Kincade* majority scolded Judge Reinhardt's dissent for its "alarmist tone and obligatory references to George Orwell's *1984*," *see Kincade*, 379 F.3d at 835, his warning that if "the expansion of the DNA Act's reach continues to follow its current trajectory, it will not be long before CODIS includes DNA profiles from . . . all newborns" may soon bear fruit. *Kincade*, 379 F.3d at 849 (Reinhardt, J., dissenting).

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.

2010 *available at* http://articles.chicagotribune.com/2010-05-11/business/ct-biz-0512-genetic-tests-20100511_1_genetic-test-kits-walgreens (last visited July 23, 2011). While the program was shelved and led to an FDA investigation and congressional hearing, it is still possible to purchase genetic tests over the Internet. *See* https://www.23andme.com/ (offering genetic tests for $99) (last visited July 23, 2011).

[21] 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*, *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 July 23, 2011).

Lewis, et al., *State Laws Regarding the Retention and Use of Residual Newborn Screening Blood Samples*, Pediatrics 2011; 127; 703-712, at 704 (March 28, 2011)[22] (hereinafter "*Newborn Blood Screening Laws*"). Hospitals collect a small blood sample from each newborn within the first 24 hours of his or her life and send it to testing for rare genetic, congenital and functional disorders. After testing, state rules vary widely on what the state may or must do with the sample, *id.* at 706-707 (table of state laws), but 40% of states retain the sample for at least a year. *Id.* at 704

While newborn genetic screenings are important, have contributed to advances in research, prevented thousands of serious health consequences, and saved lives, *id.* at 707, the national collection program has not been without controversy. In 2009, after litigation and several public records requests, it was revealed that the Texas Department of State Health Services ("DSHS") stored newborn blood spots indefinitely and used and shared them with others for research purposes without parental consent. *See Beleno, et al v. Texas Department of State Health Services, et al*, 5:09-CV-00188 (W.D. Tx. 2009). In one of the most controversial instances of sharing, Texas DSHS distributed hundreds of maternally unrelated bloodspots to the U.S. Armed Forces Pathology Laboratory for use in a forensic mitochondrial DNA (mtDNA) registry. *See* Emily Ramshaw,

[22] *Also available at* http://www.genomicslawreport.com/wp-content/uploads/2011/04/Pediatrics_newborn-screening.pdf (last visited July 23, 2011).

"DSHS Turned Over Hundreds of DNA Samples to Feds," *Texas Tribune*, February 2, 2010.[23] This database was built specifically to solve crimes, identify missing persons, and eventually, to allow mtDNA to be shared internationally for law enforcement and anti-terrorism purposes. *Id.* As a result of the controversy surrounding Texas's blood spot collection program, the agency ultimately destroyed all samples it collected before May 2009—nearly 5 million samples in all. *Id.*; *see also* Texas DSHS, Statement: Newborn Screening Settlement News Release (Dec. 22, 2009).[24]

The situation in Texas highlights the potential for abuse inherent in DNA collection programs. As noted, many states retain residual blood spots collected from newborns for at least a year, and some states, including California, may retain the bloodspots for up to 21 years unless a parent specifically requests its destruction.[25] While some states have attempted to draft clear laws regarding who may access the samples and for what purposes, *see* Lewis, *et al*. *Newborn Blood*

---

[23] *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 July 23, 2011).

[24] *Available at* http://www.dshs.state.tx.us/news/releases/20091222.shtm (last visited July 23, 2011).

[25] California's newborn screening statutes and regulations do not discuss how long the state may retain samples. *See* Cal. Health & Safety Code §§ 125000-125002; 124975-124996. However, the department of public health has indicated it may retain samples for up to 21 years. *See* California Department of Public Health, *Notice of Information and Privacy Practices*, Genetic Disease Screening Program, Newborn Screening Branch, *available at* http://www.cdph.ca.gov/programs/GDSP/Documents/Privacy%20Policy.pdf (last visited July 23, 2011).

Screening Laws at 705-707, even the clearer laws allow room for interpretation. For example, after Texas's newborn blood sample sharing controversy and resulting statutory changes, a Texas DSHS spokeswoman stated the Armed Forces study fell "under the broader category of public health research."[26] Equating sharing for forensics and law enforcement purposes and sharing for research to discover a cure for cystic fibrosis strains the definition of "public health" and opens the door for even broader sharing.

It remains to be seen whether other states will attempt to broaden their sharing of newborn blood samples or whether law enforcement may try to regularly access this data in the future.[27] However, given the massive DNA collection occurring in other contexts, including from arrestees under the DNA Act at issue in this case, these risks cannot be ignored.

III. CONCLUSION

The panel's unprecedented acceptance of warrantless and suspicionless DNA testing from all arrestees is the unfortunate next step towards a future where "all Americans will be at risk . . . of having our DNA samples permanently placed

[26] *See* Mary Ann Roser, "Suit Possible Over Baby DNA Sent to Military Lab for National Database," *Austin American-Statesman,* February 22, 2010, *available at* http://www.statesman.com/news/texas-politics/suit-possible-over-baby-dna-sent-to-military-268714.html (last visited July 23, 2011).

[27] It is easy to imagine a situation where, in a state that stores newborn blood samples for 21 years or indefinitely, law enforcement might want access to blood samples to connect a suspect whose DNA is not yet in CODIS with a crime where DNA has been collected at the scene of a crime.

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).

"The time to put the cork back in the brass bottle is now—before the genie escapes." *Kincade*, 379 F.3d at 875 (Kozinski, J., dissenting). This Court should reverse the panel and find the warrantless collection of Mr. Pool's DNA violates the Fourth Amendment.

Dated: July 25, 2011

By: /s/ Hanni Fakhoury__

Hanni Fakhoury
Lee Tien
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org

Attorneys for Amici Curiae

**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 Amici Curiae In Support Of Defendant/Appellant and Reversal complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,948 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: July 25, 2011

By: /s/ Hanni Fakhoury__

Hanni Fakhoury
Lee Tien
Jennifer Lynch
ELECTRONIC FRONTIER
FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org

Attorneys for Amici Curiae

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 July 25, 2011.

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: July 25, 2011

By: /s/ Hanni Fakhoury__

Hanni Fakhoury
Lee Tien
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org

Attorneys for Amici Curiae