Case No. S196200

IN THE SUPREME COURT
OF THE STATE OF CALIFORNIA

THE PEOPLE OF THE STATE OF CALIFORNIA,
Plaintiff and Respondent,
v.
MARK BUZA,
Defendant and Appellant,

AFTER A DECISION BY THE COURT OF APPEAL
FIRST APPELLATE DISTRICT, DIVISION TWO, CASE NO. A125542
FILED AUGUST 31, 2011;
SAN FRANCISCO COUNTY SUPERIOR COURT CASE NO. 207818

APPLICATION OF THE ELECTORNIC FRONTIER FOUNDATION FOR LEAVE TO FILE *AMICUS CURIAE* BRIEF AND *AMICUS* BRIEF IN SUPPORT OF DEFENDANT AND APPELLANT MARK BUZA

ELECTRONIC FRONTIER FOUNDATION
Hanni Fakhoury (SBN 252629)
454 Shotwell Street
San Francisco, California 94109
Telephone: (415) 436-9333
hanni@eff.org
Attorney for Amicus Curiae
Electronic Frontier Foundation

APPLICATION OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION TO FILE AN *AMICUS* BRIEF IN SUPPORT OF DEFENDANT/APPELLANT MARK BUZA AND STATEMENT OF INTEREST

Pursuant to California Rule of Court 8.520(f), the Electronic Frontier Foundation ("EFF") respectfully requests leave to file an *amicus* brief in support of Defendant/Appellant Mark Buza.[1]

EFF is a San Francisco-based, donor-supported, nonprofit civil liberties organization working to protect and promote fundamental liberties in the digital world. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and courts to support free expression, privacy, and transparency in the information 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

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus* contributed money intended to fund preparing or submitting this brief.

Cir. 2011); *see also Haskell v. Harris*, 669 F.3d 1049 (9th Cir. 2012) (filed *amicus* brief in support of rehearing en banc).

For these reasons, *amicus* respectfully requests leave to file the attached brief.

DATED: June 1, 2012

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

By: Hanni Fakhoury

Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94109
Telephone: (415) 436-9333
Attorney for Amicus Curiae Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statute

State Statutes

Other Authorities

Constitutional Provisions

INTRODUCTION AND SUMMARY OF ARGUMENT

Courts and judges throughout this country have concurred with the lower court's concern that DNA samples and profiles reveal incredibly sensitive information about individuals. (*See Haskell v. Harris* (9th Cir. 2012) 669 F.3d 1049, 1079 (W. Fletcher, J., dissenting) ["Even with today's technology, however, junk DNA reveals more information than a fingerprint."]; *United States v. Pool* (9th Cir. 2010) 621 F.3d 1213, 1216, *opinion vacated* (9th Cir. 2011) 659 F.3d 761 ["[r]ecent studies have begun to question the notion that junk DNA does not contain useful genetic programming material."] (quoting *United States v. Kincade* (9th Cir. 2004) 379 F.3d 813, 818 n.6 (en banc)); *see also Pool*, *supra,* 621 F.3d at 1234 (conc. opn. of Lucero, J.) ["[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*, *supra,* 379 F.3d at 842 n.3 (conc. opn. of Gould, J.).)

And yet, the government wants 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* (2004) 533 U.S. 27, 34.) 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* (7th Cir. 2007) 474 F.3d 994, 997 (citing *Katz v. United States* (1967) 389 U.S. 347 and *Kyllo*).)

The government wants a future in which every person's DNA is sampled and profiled. As Judge Kozinski has noted, "[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*, *supra,* 379 F.3d at 872 (dis. opn. of Kozinski, J.).) At that point, every person can be "identified" at any place where he or she has been, without suspicion or a warrant.

Because the lower court appropriately balanced the government's investigative needs with the privacy rights at stake here, the appellate court's opinion should be affirmed.

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* (1973) 412 U.S. 218, 219.) "[S]earches conducted without grounds for suspicion of particular individuals have been upheld . . . in 'certain limited circumstances.'" (*Chandler v. Miller* (1997) 520 U.S. 305, 308 (quoting *Treasury Employees v. Von Raab* (1989) 489 U.S. 656, 668).)

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* (1971) 403 U.S. 443, 455.)

The government's Fourth Amendment analysis suffers from three major flaws. It (1) underscores the "intrusiveness" of the actual "search;" (2) relies on an inapplicable exception to the Fourth Amendment to justify the repeated warrantless search; and (3) ignores the significant and actual privacy interests involved.

This Court should reject the government's arguments and affirm the appellate court.

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

"The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." (*Schmerber v. California* (1966) 384 U.S. 757, 767.) 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.* (1985) 469 U.S. 325, 341.)

The government incorrectly considers the intrusion here "minimally invasive – both in terms of the bodily intrusion it occasions, and the information it lawfully produces." (ROB[1] at 33 (quoting *Kincade*, *supra*, 379 F.3d at 837-38.).) But the "intrusion" here is measured by the breadth of the government's entrance into what was previously a private sphere, and not by the physical intrusion caused by a buccal swab.

And with that concept in mind, is important to be clear about the Fourth Amendment events at issue here. DNA collection is not 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. Missing from this analysis is 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.

Rather, as many courts have done, the better approach is to disaggregate. (*See King v. State* (Md. 2012) --- A.2d ----, 2012 WL 1392636, *20 ["As other courts have concluded, we look at any DNA collection effort as two discrete and separate searches."].) First, the collection of the DNA sample, as a physical intrusion on the body of the

[1] Consistent with Buza's Answering Brief on the Merits, "ROB" refers to the Respondent's Opening Brief on the Merits.

person, is a search and a seizure. (*See id.*; *Friedman v. Boucher* (9th Cir. 2009) 580 F.3d 847, 852.) Second, the "ensuing chemical analysis of the sample to obtain physiological data" is also a search. (*Skinner v. Railway Labor Executives' Assn.* (1989) 489 U.S. 602, 616; *King*, *supra*, 2012 WL 1392636 at *20.)

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* (9th Cir. 2007) 508 F.3d 941, 956 (dis. opn. of B. Fletcher, J.) ["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*, *supra*, 379 F.3d at 873 (dis. opn. of Kozinski, J.).) To "search" means "[t]o look over or through for the purpose of finding something; to explore." (*Kyllo*, *supra,* 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*, *supra,* 379 F.3d at 873 (dis. opn. of Kozinski, J.) ["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* Paul Ohm, *The Fourth Amendment Right to Delete* (2005) 119 Harv. L. Rev. F. 10 [arguing that since "seizure" is about dispossession, an individual loses ability to delete information when the government has a copy of it].)

With this understanding of the search at issue here, it becomes clear just how "invasive" DNA collection is. And 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. Unlike a fingerprint, DNA searches involve "intrusion into the widest spectrum of human privacy." (*Pool*, *supra,* 621 F.3d at 1232 (conc. opn. of Lucero, J.); *see also Haskell, supra,* 669 F.3d at 1079 (dis. opn. of W. Fletcher, J.) ["our more recent decisions have explicitly recognized that DNA testing constitutes a greater infringement on privacy than fingerprinting."].)

Judge Rendell of the Third Circuit has warned, an "intact, unanalyzed DNA sample contains a vast amount of sensitive information" beyond simply "the individual's identity, including familial lineage and predisposition to over four thousand types of genetic conditions and diseases and, potentially, genetic markers for traits including aggression, sexual orientation, substance addiction, and criminal tendencies." (*United*

States v. Mitchell (3d Cir. 2011) 652 F.3d 387, 424 (dis. opn. of Rendell, J.) (quotations and citations omitted).)

And Judge Reinhardt of the Ninth Circuit has noted DNA evidence can capture a person – and his or her relatives' – medical history, including "genetic defects, predispositions to diseases, and perhaps even sexual orientation." (*Kincade*, *supra*, 379 F.3d at 850 (dis. opn. of Reinhardt, J.) (quoting Harold J. Kent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment* (1995) 74 Tex.L.Rev. 49, 95-96 (quotations omitted)).)

Since DNA searches are far more intrusive than a fingerprint, it is clear the appellate court's decision finding these warrantless searches in violation of the Fourth Amendment is correct.

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

The government's argument that the "malleable and boundless" totality of the circumstances test justifies the warrantless and suspicionless seizure and repeated search of a pretrial arrestee's DNA is wrong because this analysis simple does not apply here. (*Kincade, supra,* 379 F.3d at 860 (dis. opn. of Reinhardt, J.); *see also* ROB at 30.)

The Fourth Amendment only allows searches unsupported by individualized suspicion in "certain limited circumstances." (*Von Raab*, *supra*, 489 U.S. at 668). These exceptions include, "special needs" searches

conducted for non-law enforcement purposes. (*See City of Indianapolis v. Edmond* (2000) 531 U.S. 32, 37). Numerous Courts have already found the "special needs" approach cannot be used to justify warrantless DNA collection because it is intended for law enforcement purposes. (*See Haskell*, *supra,* 669 F.3d at 1054; *Mitchell*, *supra,* 652 F.3d at 403; *King, supra,* 2012 WL 1392636 at *5.)

Another of these "limited circumstances" is probation and parole searches. (*See United States v. Knights* (2001) 534 U.S. 112; *Samson v. California* (2006) 547 U.S. 843 (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*, *supra,* 547 U.S. at 848 (quoting *Knights*, *supra*, 534 U.S. at 118).) In both cases, the Court noted that a person's status as a convicted felon is "salient." (*Samson*, *supra,* 547 U.S. at 848 (quoting *Knights*, *supra,* 534 U.S. at 118).

In prior cases addressing the constitutionality of DNA collection, 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*, *supra*, 379 F.3d at 833; *Kriesel*, *supra,* 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*, *supra*, 508 F.3d at 944; *Kincade*, *supra*, 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." (*Kincade, supra,* 379 F.3d at 834-35; *see also Kriesel*, *supra*, 508 F.3d at 949.)

The government, however, seeks to create a new dividing line by applying this totality of the circumstances test to persons who are mere arrestees. (ROB 50-54.) Some courts to address the issue have justified the DNA collection of a mere arrestee by relying on the "totality of the circumstances" test in *Samson* and *Knights*. (*See Haskell, supra,* 669 F.3d at 1054, *Mitchell, supra,* 652 F.3d at 403.) But these courts are wrong because a mere arrestee is not the constitutional equivalent of a convicted person.

The Supreme Court in *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.'" (*Samson, supra,* 547 U.S. at 848 (quoting *Knights, supra,* 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*, *supra,* 547

U.S. at 850.) The Supreme Court ruled that since both probationers and parolees have been *convicted*, the interests of preventing recidivism by convicted felons justify a suspicionless search. (*Id.* at 853-54; *Knights*, *supra,* 534 U.S. at 120-21.)

But an arrestee "has great privacy interests than someone who has been convicted." (*Haskell, supra,* 669 F.3d at 1078 (dis. opn. of Fletcher, W.).) Arrestees even possess "far greater" privacy interests than a person on probation because they are "are ordinary people who have been accused of a crime but are presumed innocent." (*United States v. Scott* (9th Cir. 2006) 450 F.3d 863, 871-73.)

Moreover, the Supreme Court has never "ruled that law enforcement officers may conduct suspicionless searches on pretrial detainees for reasons other than prison security." (*Friedman*, *supra,* 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* (1979) 441 U.S. 520, there was a non-law enforcement interest in the search: recidivism and prison security. *See Haskell*, *supra,* 669 F.3d at 1078 (dis. opn. of W. Fletcher, J.).) But collecting and searching DNA only serves the government's interest in law enforcement investigation.[2]

[2] 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

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 of 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, supra,* 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, the Court of Appeal was correct in finding it violated the Fourth Amendment.

C. The Privacy Interests at Stake Are Not Speculative, But Significant and Real.

The government believes that the appellate court was speculating about "hypothetical uses that have not come to pass" in finding warrantless DNA collection unconstitutional. (ROB at 41, 43.)

But the Supreme Court has explained "the rule [a court] adopts must take account of more sophisticated systems that are already in use or in *development*." (*Kyllo, supra,* 533 U.S. at 36 (emphasis added).) And courts "should not be blind to the potential for abuse when assessing the legitimacy" of DNA collection." (*Mitchell, supra*, 652 F.3d at 424 (dis. opn. of Rendell, J.).) This Court cannot avoid confronting the "legitimate

---

permitted. (*Scott, supra,* 450 F.3d at 872 n. 11). It is doubtful whether collecting DNA furthers that interest. (*See Kriesel, supra,* 508 F.3d at 957 (dis. opn. of B. Fletcher, J).)

and real" privacy implications of a rapidly evolving technology that is being used forensically. (*Id.*)

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 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 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, 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* (2012) 132 S. Ct. 945, 963 (conc. op. of Alito, J.).) But as *Jones* itself demonstrated, today's technology has made government surveillance easier, and in turning making it potentially more routine. (*Jones, supra*, 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* (1976) 425 U.S. 435.) 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. As Justice Sotomayor commented in her concurring opinion in *Jones*,

> 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.

(*Jones*, *supra,* 132 S.Ct. at 957 (conc. opn. of Sotomayor, J.).) But the conclusion is inescapable: cost 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.[3]

This same 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"[4] DNA sequencing technology will mean that "DNA sequencing costs will no longer be a factor limiting personal human genomics technologies."

---

[3] JASON (The MITRE Corporation), *The $100 Genome: Implications for the DoD* (Dec. 15, 2010) at p. 11, available at <www.fas.org/irp/agency/dod/jason/hundred.pdf> (as of May 30, 2012) (hereinafter "JASON Report").

[4] The JASON report explains "new technologies, called third-generation sequencing systems," are expected to account for this cost reduction. (JASON Report, *supra,* 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.)

(JASON Report 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, then there will be no legal constraint on government collection of our DNA from public places. (*See* Jules Epstein, *"Genetic Surveillance"—The Bogeyman Response to Familial DNA Investigations* (2009) 2009 U. Ill. J.L. Tech. & Pol'y 141, 151.) 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 and to Build a Bigger Biometric Database.

Dissenting judges have warned of a "slippery slope toward ever-expanding warrantless DNA testing." (*Pool, supra*, 621 F.3d at 1235 (dis. opn. of Schroeder, J.) [citing *Kincade, supra*, 379 F.3d at 842-71 (dis. opn. of Reinhardt, J.) and 871-75 (dis. opn. of Kozinski, J)].) These dissents were prescient. The government's collection, sharing and analysis of DNA profiles and other biometric identifiers has expanded significantly over the last few years.

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.[5] As of April 2012, the National DNA Index (where California sends its DNA samples) contains over 10,718,700 offender profiles, and states' individual databases are each expanding as well.[6]

Some have predicted even greater 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).[7] As DHS may detain "non-United States persons" for

---

[5] Marc Nelson, *Making Sense of DNA Backlogs, 2010—Myths vs. Reality*, (Feb. 2011) National Institute of Justice, p. 7–8 <http://www.ncjrs.gov/pdffiles1/nij/232197.pdf> (as of May 30, 2012).

[6] FBI, "CODIS—NDIS Statistics," <http://www.fbi.gov/about-us/lab/codis/ndis-statistics> (as of May 30, 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 <http://oag.ca.gov/sites/all/files/pdfs/bfs/quarterlyrpt.pdf (as of May 30, 2012). As of December 31, 2011, California has 1,930,306 DNA profiles in its database. (*Id.*)

[7] *See* Jennifer Lynch, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond* (May 2012), Electronic Frontier Foundation, <https://www.eff.org/sites/default/files/filenode/BiometricsImmigration052112.pdf > (as of May 30, 2012).

purely civil rather than law enforcement purposes, such as overstaying a visa, it has been estimated by DHS that this this could affect over a million people annually, including juveniles.[8]

Current 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, *supra, 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.[9]

To meet these demands, the DOJ has spent the last five years attempting to "re-architect the CODIS software" to expand its capabilities.[10] 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

---

[8] *See* Lynch, *supra,* at p. 7.

[9] *See* Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 Stan L. Rev. 751 (Apr. 2011) 764-65 (noting the current version of CODIS "is poorly designed for identifying true leads where partial matches are uncovered").

[10] *See* FBI, "CODIS—The Future." <http://www.fbi.gov/about-us/lab/codis/codis_future> (as of May 30, 2012).

matching process."[11] While the current status of Next Generation CODIS is unclear,[12] the DOJ has stated it plans to roll out a new version of CODIS sometime in 2011-2012.[13] 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. It will also allow greater interoperability with state and international DNA databases. This report and the FBI's own website also state that the DOJ will introduce further improvements to CODIS in the near future, including

---

[11] *See* Unisys, "FBI Contracts with Unisys for Development and Deployment of Next-Generation Combined DNA Index System." <https://www.unisys.com/products/news_a_events/all__news/10198717.htm (as of May 30, 2012).

[12] 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. (FBI, "Next Generation Identification" <http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi> (as of May 30, 2012).) 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) <http://ccrjustice.org/newsroom/press-releases/new-documents-reveal-behind-scenes-fbi-role-controversial-secure-communities-deportation-program> (as of May 30, 2012).)

[13] *See* Department of Justice, *Exhibit 300: Capital Asset Plan and Business Case Summary, FBI Combined DNA Index System* (2011) p. 1 <http://www.justice.gov/jmd/2011justification/exhibit300/fbi-2011-cjis-wan.pdf> (as of May 30, 2012).

"expanding CODIS capabilities in terms of DNA match technologies (*e.g.* electropheragram, base composition, full mtDNA sequence, mini-STRs, SNPs)" and kinship searches.[14]

As shown above, the "slippery slope toward ever-expanding warrantless DNA testing" dissenting judges have predicted, is not speculation, but already upon us. *(Kincade, supra*, 379 F.3d at 842-71 (dis. opn. of Reinhardt, J.).)

3. DNA Collection is Already Expanding in Non-Forensic Contexts.

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,[15] to personal DNA testing,[16] to blood and tissue samples collected for public health purposes.

---

[14] *See also* FBI, "CODIS—The Future," <http://www.fbi.gov/about-us/lab/codis/codis_future> (as of May 30, 2012) [noting the re-architecture of CODIS will allow it "to include additional DNA technologies."].

[15] 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, *supra,* at 50.) In 2011, the Army issued a solicitation suggesting it may plan to follow JASON's recommendations. (U.S. Army, *Archive of Samples for Long-term Preservation of RNA and Other Nucleic Acids* (2011) Small Business Innovation Research Program, <http://www.dodsbir.net/sitis/archives_display_topic.asp?Bookmark=40675 (as of May 30, 2012).)

[16] In 2010, 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, 2010

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[17] 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. In 2004, one federal circuit judge warned 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." (*Kincade, supra*, 379 F.3d at 849 (dis. opn. of Reinhardt, J.) That thought may soon bear fruit.

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.[18]

<http://articles.chicagotribune.com/2010-05-11/business/ct-biz-0512-genetic-tests-20100511_1_genetic-test-kits-walgreens (as of May 30, 2012). 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 $299) (as of May 30, 2012).

[17] 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*, <http://www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/5.-US-Veterans-Affairs-25-30-million> (as of May 30, 2012).

[18] *See* Michelle H. Lewis, *et al*., *State Laws Regarding the Retention and Use of Residual Newborn Screening Blood Samples* (March 28, 2011) *Pediatrics 2011*; 127; 703-712, at 704

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, but 40% of states retain the sample for at least a year.[19]

While newborn genetic screenings are important, have contributed to advances in research, prevented thousands of serious health consequences, and saved lives,[20] 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.[21] 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.[22]

<http://www.genomicslawreport.com/wp-content/uploads/2011/04/Pediatrics_newborn-screening.pdf> (as of May 30, 2012) (hereinafter "*Newborn Blood Screening Laws*").

[19] *(Id.* at 706-707 [table of state laws].)

[20] *(Id.* at 707.)

[21] *See Beleno, et al. v. Texas Department of State Health Services, et al.*, 5:09-cv-00188 (W.D. Tx. 2009).

[22] *See* Emily Ramshaw, "DSHS Turned Over Hundreds of DNA Samples to Feds," *Texas Tribune*, February 2, 2010 <http://www.texastribune.org/texas-state-agencies/department-of-state-health-services/dshs-turned-over-hundreds-of-dna-samples-to-feds/#> (as of May 30, 2012).

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. 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.[23]

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.[24] While some states have attempted to draft clear laws regarding who may access the samples and for what purposes, even the clearer laws allow room for interpretation.[25] For example, after Texas's newborn blood sample sharing controversy and

---

[23] *See* Texas DSHS, Statement: Newborn Screening Settlement News Release (Dec. 22, 2009). <http://www.dshs.state.tx.us/news/releases/20091222.shtm> (as of May 30, 2012).

[24] 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.) 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, <http://www.cdph.ca.gov/programs/GDSP/Documents/Privacy%20Policy.pdf> (as of May 30, 2012).

[25] *See* Lewis, *supra, Newborn Blood Screening Laws* at 705-707,

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 with 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 real risks cannot be ignored as hypothetical speculation.

CONCLUSION

The government's desire for 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

---

[26] *See* Mary Ann Roser, "Suit Possible Over Baby DNA Sent to Military Lab for National Database," *Austin American-Statesman* February 22, 2010 <http://www.statesman.com/news/texas-politics/suit-possible-over-baby-dna-sent-to-military-268714.html> (as of May 30, 2012).

[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 DNA collected at a crime scene.

suspicionless searches conducted for law enforcement purposes." (*Kincade, supra*, 379 F.3d at 843 (dis. opn. of Reinhardt, J.).)

This is not merely a "parade of horribles" but the road we are presently on. (*Haskell, supra,* 669 F.3d at 1063.) In 2004, Judge Kozinski warned that "the time to put the cork back in the brass bottle is now—before the genie escapes." (*Kincade, supra,* 379 F.3d at 875 (dis. opn. of Kozinski, J.). Too many courts ignored this warning, and inevitably, DNA collection has rapidly expanded in the last eight years.

For heeding this advice and finding that warrantless DNA collection from innocent individuals, people arrested but not yet convicted, violates the Fourth Amendment, this Court should affirm the decision of the Court of Appeals.

DATED: June 1, 2012

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

By: Hanni Fakhoury

Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94109
Telephone: (415) 436-9333
hanni@eff.org
Attorney for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

Counsel for *Amicus Curiae* hereby certifies, pursuant to Rule 8.204(c) of the California Rules of Court, that the enclosed brief was produced using 13-point type, including footnotes, and contains approximately 5,846 words, which is less than the 14,000 words permitted by this rule. Counsel relies on the word count of the computer program used to prepare this brief.

Dated: June 1, 2012

By: Hanni Fakhoury

Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94109
Telephone: (415) 436-9333
Attorney for Amicus Curiae Electronic Frontier Foundation

PROOF OF SERVICE

I, Stephanie Shattuck, declare that I am employed in the city and county of San Francisco, California. My business address is 454 Shotwell Street, San Francisco, California 94110. I am over the age of eighteen years and am not a party to the within cause.

On June 1, 2012, I served the attached APPLICATION OF THE ELECTORNIC FRONTIER FOUNDATION FOR LEAVE TO FILE *AMICUS* CURIAE BRIEF AND *AMICUS* BRIEF IN SUPPORT OF DEFENDANT/APPELLANT MARK BUZA on the interested parties in said cause by:

X U.S. Mail: placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in accordance with the firm's practice of collection and processing correspondence with the United States Postal Service, which in the normal course of business provides for the deposit of all correspondence and documents with the United States Postal Service on the same day they are collected and processed for mailing to the person(s) at the address(es) set forth below:

Enid A. Camps Office of the Attorney General 455 Golden Gate Avenue, Suite 11000 San Francisco, CA 94102	James Bradley O'Connell Kathryn Seligman First District Appellate Project 730 Harrison Street, Suite 201 San Francisco, CA 94107
Attorneys for Plaintiff/Respondent	*Attorneys for Defendant/Appellant*

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATED: June 1, 2012

_____

STEPHANIE SHATTUCK