Universal DNA databases: a way to improve privacy?

Kirsten Dedrickson*

Stanford Law School, Stanford University, Stanford, CA 94305-8610, USA
Corresponding author. E-mail: kdedrick@stanford.edu

KEYWORDS: database, DNA, genetic, invasion, privacy, universal

[A comprehensive DNA database] would entail but a limited intrusion on individual freedom and privacy while advancing both public safety and racial even-handedness in the criminal justice system and serving as a firewall against far greater intrusions on privacy by law enforcement authorities.

– Kaye & Smith¹

INTRODUCTION

Many people have a visceral, negative reaction to the idea of a universal DNA database. Their main concern? That a universal DNA database would grossly invade their privacy.

A universal DNA database’s benefits in efficiently and effectively solving crimes, exonerating the innocent, and decreasing racial disparities in law enforcement, however, make such a database immensely appealing from a public safety and criminal justice perspective. As of April 2017, the federal DNA database has assisted in more than 358,069 investigations.² DNA evidence has exonerated 350 innocents who combined had served 4787 years in prison, sometimes on death row.³ DNA also enabled law enforcement to identify 149 of the true perpetrators of those crimes, who ‘went on to

* Kirsten Dedrickson has a bachelor’s degree in philosophy and computer science from Dickinson College, and is expected to graduate from Stanford Law School with a J.D. in 2018.

¹ David H. Kaye & Michael E. Smith, DNA Identification Databases: Legality, Legitimacy, and the Case for Population-wide Coverage, 2003 Wis. L. Rev. 413, 440 (2003).

² Federal Bureau of Investigation, CODIS – NDIS Statistics, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (accessed July 1, 2017).

³ Innocence Project, DNA Exonerations in the United States, https://www.innocenceproject.org/dna-exonerations-in-the-united-states/ (accessed July 1, 2017).
be convicted of 147 additional violent crimes, including 77 sexual assaults, 35 murders, and 35 other violent crimes while the innocent sat behind bars for their earlier offenses. A universal DNA database could have prevented those 350 false convictions and 147 later violent crimes.

Yet discussions about universal databases are often halted by invasion of privacy concerns. Are those concerns rational? By analysing a universal DNA database’s design, the probability that imagined abuses would occur, and the invasive investigative techniques the database could end, this article demonstrates that a universal DNA database might actually improve privacy.

Part I briefly introduces current forensic DNA databases. Part II examines how a universal DNA database could be designed to limit its privacy-invasion potential. Part III responds to common privacy-based objections. Finally, Part IV argues that a universal DNA database may even increase privacy by decreasing more invasive investigative techniques, exonerating the innocent, and deterring crime. While constitutional arguments may exist on this topic, space does not allow their consideration here.

I. Current DNA Databases

DNA databases are already maintained by every state and the federal government. All states require DNA samples to be taken from individuals convicted certain crimes. Twenty-nine states and the federal government even collect DNA from individuals arrested, but not yet convicted, for certain offenses. All states have some process for expunging DNA profiles if a charge is dropped or the individual is acquitted, though most states require individuals to initiate the process. Only 36 per cent of state DNA profiles are incorporated into the national Combined DNA Index System (CODIS) database.

After obtaining DNA from an offender or arrestee, law enforcement sends the DNA to an accredited, quality-controlled forensic laboratory. The laboratory then examines the 13 ‘CODIS loci’, also known as ‘CODIS markers’, of the DNA. Combined, the CODIS loci comprise only one millionth of a person’s DNA and are ‘no more informative than an ordinary fingerprint’. These ‘noncoding, nonregulatory’ snippets of DNA are not ‘even moderately correlated with disease status, physical traits, or behavioral predispositions’. Analysing these portions of an individual’s ‘junk’ DNA thus ‘produces a set of numbers that are useful for identification purposes and

---

4 Id.
5 See DNA Resource, State DNA Database Laws Qualifying Offenses (As of Sept. 2011), http://www.dnaresource.com/documents/statequalifyingoffenses2011.pdf.
6 See NDIS Statistics, supra note 2.
7 National Institute of Justice, DNA Sample Collection from Arrestees (Dec. 7, 2012) https://www.nij.gov/topics/forensics/evidence/dna/pages/collection-from-arrestees.aspx.
8 Cronan, supra note 7, at 137 (2000).
9 See Federal Bureau of Investigation, Frequently Asked Questions on CODIS and NDIS, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (accessed July 1, 2017).
10 David H. Kaye, Two Fallacies About DNA Data Banks for Law Enforcement, 67 BROOK. L. REV. 179, 188 (2001).
11 Kaye & Smith, supra note 1, at 431.
12 Id.
13 Brief of Genetics, Genomics & Forensic Science Researchers as Amici Curiae in Support of Neither Party, Maryland v. King, 133 S. Ct. 1958 (2013) (No. 12-207), 2012 WL 6762585, at *2 [hereinafter Maryland v. King Amicus Brief].
nothing else’.\textsuperscript{14} These numbers become the offender or arrestee’s DNA profile.\textsuperscript{15} CODIS does not store any personally identifying information with a DNA profile, not even the name of the person who provided the DNA sample or that sample itself.\textsuperscript{16} If a DNA sample taken from a crime scene matches a CODIS profile, a public forensic laboratory must contact the other laboratories involved in creating the DNA profile to obtain the suspect’s name.\textsuperscript{17}

In addition to limiting the information stored in DNA databases, current databases also strictly limit access and use of that information. All CODIS computers are ‘located in [a] physically secure space’ and laboratory communications occur over a private network ‘accessible to only criminal justice agencies approved by the FBI.’\textsuperscript{18} Generally, access to the databases is strictly limited to criminal justice agencies ‘for law enforcement purposes’,\textsuperscript{19} that is, criminal identification only.\textsuperscript{20} Criminal defendants may also be given access to samples and analyses connected to their cases.\textsuperscript{21} Unauthorized tampering, acquisition, disclosure, or use of DNA profiles is subject to fines and prosecution.\textsuperscript{22}

\section*{II. Limiting a Universal DNA Database’s Privacy-Invasion Potential}

A universal DNA database could be designed very similarly to current DNA databases, none of which have been declared unreasonable invasions of privacy. Only three changes are necessary to create a universal database: (i) include all individuals, not just those convicted or arrested for qualifying offenses; (ii) repeal profile expungement laws; and (iii) better integrate or combine existing databases.

As explained above, current databases implement many privacy protections. DNA profiles store only numerical representations of ‘junk’ DNA which can identify an individual, but cannot reveal any information about that person’s health, physical appearance, or behavioral predispositions. The DNA profiles are stored in physically secured locations with limited access and the related names are stored separately to prevent tampering and misuse. Finally, database abuses are discouraged through fines, criminal charges, and possible jail time.

A universal DNA database can, and should, maintain these privacy protections. Additional protections could also be implemented.

Perhaps most importantly, DNA samples could be destroyed immediately after a DNA profile is generated and use of the samples for any other purpose could be

\begin{footnotesize}
\textsuperscript{14} David H. Kaye, Bioethical Objections to DNA Databases for Law Enforcement: Questions and Answers, 31 Seton Hall L. Rev. 936, 943 (2001).
\textsuperscript{15} CODIS FAQs, supra note 9.
\textsuperscript{16} Id. Conversely, almost every state retains samples indefinitely. Mark A. Rothstein & Meghan K. Talbott, The Expanding Use of DNA in Law Enforcement: What Role for Privacy?, 34 J.L. Med. & Ethics 153, 158 (2006).
\textsuperscript{17} Sheldon Krimsky & Tania Simoncelli, Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties 31–32 (2011).
\textsuperscript{18} CODIS FAQs, supra note 9.
\textsuperscript{19} Id. Some states also allow access for humanitarian purposes. See Id.
\textsuperscript{20} Paul M. Monteleoni, DNA Databases, Universality, and the Fourth Amendment, 82 N.Y.U. L. Rev. 247, 257 (2007).
\textsuperscript{21} CODIS FAQs, supra note 9.
\textsuperscript{22} Natalie A. Bennett, A Privacy Review of DNA Databases, 41/S: J. L. & Pol’y for Info. Soc’y 821, 835.
\end{footnotesize}
criminally sanctioned.\textsuperscript{23} This would prevent future testing of the samples for private information such as disease status or behavioral predispositions. Indeed, ‘an instrument could be built that would extract an identifying profile and destroy the sample at the same time’ to ensure that does not happen.\textsuperscript{24} If implemented and enforced, a sample destruction policy would help ensure nothing more than a genetic fingerprint is taken from someone’s DNA. For this reason, sample destruction has been hailed as not only ‘[t]he best way to mitigate [] privacy concerns’,\textsuperscript{25} but perhaps even ‘[t]he solution to the privacy problem’.\textsuperscript{26}

DNA profiles could also be generated anonymously.\textsuperscript{27} Rather than sending a DNA sample to a lab with the related name, the collecting agency could generate a random sample identification number associated with the name and DNA profile. The agency could then send the sample to a certified lab to generate the CODIS profile, and separately send the name to an independent agency holding a ‘master list’ of individuals represented in the database.\textsuperscript{28} This system would decrease the likelihood of unauthorized tests occurring and, even if such testing did occur, help ensure the results could not be linked or undesirably disclosed to the DNA’s source. This system also makes the names easier to secure and maintain by (a) making it harder for thieves to steal usable information, and (b) limiting the number of storage locations potentially vulnerable to theft, error, or closure.\textsuperscript{29} It may even be feasible to protect the names and profiles from hacking by storing them on offline computers.\textsuperscript{30}

Additionally:

\begin{quote}
\textit{[t]his two-tiered system would afford significant individual privacy protection by ensuring that an administrator of the databank could never access a person’s genetic information just by knowing the person’s identity. Rather, personal information would only be revealed if that person’s DNA matches evidence found at a crime scene.}\textsuperscript{31}
\end{quote}

\begin{footnotes}
\textsuperscript{23} The Human Genetics Commission has determined there is no need for long-term retention of DNA samples. HUMAN GENETICS COMMISSION, NOTHING TO HIDE, NOTHING TO FEAR? 70 (2009), http://www.statewatch.org/news/2009/nov/uk-dna-human-genetics-commission.pdf. Indeed, Germany has already adopted these privacy protections. KRIMSKY & SIMONCELLI, supra note 17, at 210.

\textsuperscript{24} Kaye & Smith, supra note 1, at 438. The fact that ‘[m]ost police laboratories are not [even] equipped to do more invasive testing’ should also comfort those concerned about police testing more than the CODIS loci. Rychlak, supra note 23, at 254 (internal quotation marks omitted).

\textsuperscript{25} Tania Simoncelli, Dangerous Excursions: The Case Against Expanding Forensic DNA Databases to Innocent Persons, 34 J.L. MED. & ETHICS 390, 392 (2006).

\textsuperscript{26} Michael E. Smith, Let’s Make the DNA Identification Database as Inclusive as Possible, 34 J.L. MED. & ETHICS 385, 388 (2006).

\textsuperscript{27} In Germany, for example, samples are analysed without the related name ‘in a laboratory that is not connected to the investigating agency’. KRIMSKY & SIMONCELLI, supra note 17, at 211.

\textsuperscript{28} Monteleoni, supra note 20, at 258; see also, Cronan, supra note 8, at 142.

\textsuperscript{29} Cf. GENEWATCH U.K., DNA DATABASES AND HUMAN RIGHTS 12 (2011) (‘Access to DNA samples and to the DNA database must be restricted to a small number of authorized persons if security breaches are not to occur.’).

\textsuperscript{30} Cf. Christine Rosen, Liberty, Privacy, and DNA Databases, THE NEW ATLANTIS, Spring 2003, at 47 (‘The Molecular Genealogy Research Project’s ‘database is not linked to the Internet, thus avoiding the potential intrusion of computer hackers.’).

\textsuperscript{31} Cronan, supra note 8, at 142.
\end{footnotes}
A court order could also be required to obtain that person’s name to ‘ensure that law enforcement officers sought an individual’s identity for a legitimate reason’. Additional rules could be developed to regulate options when no complete match is found or when information is requested for humanitarian purposes, such as locating a missing child.

Training and enforcement programs can also be established to ensure the universal DNA database remains as private and secure as possible. DNA sample collectors, labs, law enforcement, and others involved in creating and using the DNA database can be trained on the importance of keeping the database private and how best to achieve that goal. Agencies and laboratories could be required to meet minimum national privacy and proficiency standards to participate in the creation and use of DNA profiles, and their compliance with the standards could be overseen by an independent review board. Lastly, sanctions for unauthorized testing, use, access, or distribution of DNA samples, DNA profiles, or the list of names could be further developed and enforced by an independent accountability board.

Finally, discussions about creating a universal DNA database will likely garner much political attention and contention because abuses of a universal database could affect anyone, not just criminals. Hence, ‘[p]aradoxically, a carefully constructed and administered population-wide data base may offer the greatest privacy protection for all of us by forcing the legislative and executive branches to take the greatest care in fashioning and implementing the system so as to protect privacy’.

A universal DNA database with the suggested privacy safeguards would be well protected against abuses, manipulation, and theft. While there is a risk some of these privacy protections could be circumvented with considerable effort, ‘we do not normally ban a technology due to the fear that no law can prevent’ its misuse, and in fact we have adopted beneficial technologies that pose significantly greater dangers to privacy than a universal DNA database.

III. How Much Privacy Would You Lose?—Responding to Concerns

Even with the privacy protections described above, skeptics may still worry about a universal DNA database invading their privacy. This is likely at least partially because DNA has ‘been culturally endowed with a power and significance exceeding that of other medical information’. But ‘[m]uch of this significance is undoubtedly misplaced’. Correcting the common misconception that ‘we are our DNA’ should reduce privacy-based concerns.

Nevertheless, some may still have an instinctive aversion to universal DNA databases. This part will respond to some of the most commonly raised privacy

---

32 Monteleoni, supra note 20, at 259.
33 Cronan, supra note 8, at 141.
34 Mark A. Rothstein & Sandra Carmahan, Legal & Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks, 67 BROOK. L. REV. 127, 163 (2001).
35 Krimsky & Simoncelli, supra note 17, at 159.
36 Kaye, supra note 10, at 206.
37 Monteleoni, supra note 20, at 259 n.67 (using wiretapping as an example).
38 George Annas, Genetic Privacy, 344, http://www.sjsu.edu/people/steven.lee/courses/FS169/s1/07annas.pdf.
39 Id.
objections. One commentator has denounced such concerns as fantasies: ‘As I see it, the scenarios for misuse by the government, insurers, or employers of the [CODIS-loci]-identification profiles in the NDIS and other law enforcement databases border on science fiction’. 40 This part does not go that far. But it should demonstrate that we would not sacrifice as much privacy as many assume through the adoption of a universal database.

A. Information Stored in CODIS Markers

Some opponents worry that ‘junk’ DNA may not be ‘junk’, and that the fingerprint comparison may therefore be misleading; 41 ‘some markers now thought to be meaningless may be (and have been) found to contain predictive medical information’. 42 Scientists are confident that the CODIS loci do not cause disease, but there are correlations between some loci and disease-causing genes. 43 Even with these correlations, however, the CODIS markers reveal very little about an individual. An entire DNA sample, or at least its coding portions, must be examined to learn anything meaningful about an individual’s health or appearance. 44 Indeed, ‘[i]t is unlikely that analysis of DNA profiles will ever reveal a great deal of information’ because the ‘profile represents such a small percentage of a person’s genetic code’. 45 Moreover, because the CODIS loci cannot ‘be exploited to produce a valid and useful disease-screening test’, 46 it is unlikely resources would be wasted attempting to find more correlations.

CODIS markers also cannot reveal meaningful, private information about an individual’s ethnicity or race. It is possible to use a DNA profile ‘to calculate probabilities that someone would be described as Caucasian, African-American, or Hispanic’, 47 but such inferences ‘would not be very accurate’ 48 or useful because the probabilities are based on features unrelated to characteristics typically associated with race, like skin color. 49 Regardless, such analysis is unlikely to occur or reveal sensitive information because the DNA source’s ‘apparent race would be known’ when the profile was created. 50

Furthermore, even ordinary fingerprints can ‘be correlated with perceived ethnicity or even disease or behavioral characteristics. It is simply that we, as a society, have chosen not to make much of these correlations’. 51 Hence, the fingerprint analogy conveys not only that both fingerprints and CODIS markers are useful identifiers, but also that both cause no more than a miniscule invasion of privacy. Indeed, DNA profiles provide significantly larger benefits than fingerprint databases with little more of a privacy cost.

40 David H. Kaye, Please, Let’s Bury the Junk: The CODIS Loci and the Revelation of Private Information, 102 Nw. U. L. Rev. Colloquy 70, 81 (2007).
41 See eg Elizabeth E. Job, Reclaiming ‘Abandoned’ DNA: The Fourth Amendment and Genetic Privacy, 100 Nw. U. L. Rev. 857, 869–71 (2006).
42 Id. at 870.
43 Simon A. Cole, Is the ‘Junk’ DNA Designation Bunk?, 102 Nw. U. L. Rev. Colloquy 54, 59 (2007).
44 KRIMSKY & SIMONCELLI, supra note 17, at 264.
45 Monteleoni, supra note 20, at 256 n.51.
46 Kaye, supra note 40, at 72.
47 Maryland v. King Amicus Brief, supra note 13, at *36.
48 Id.
49 Id. at *35.
50 Id. at *36.
51 Cole, supra note 43, at 61.
Lastly, some worry a universal DNA database would be used to inadvertently or maliciously determine or disprove familial relationships.\textsuperscript{52} Since (in theory) the database would contain a profile of everyone, however, law enforcement would rarely have any need or desire to find a familial match to help identify a crime scene sample.\textsuperscript{53} Indeed, if the database was designed with the protections discussed above, such a search may not be possible and, even if possible, would almost certainly require authorization and a court order. Regardless, such searches are unlikely to occur because (a) unauthorized searches would be difficult, (b) familial relationships are more easily tested by obtaining DNA samples directly from the persons of interest, and (c) most family relationships are already public knowledge.

\textbf{B. Genetic ‘Surveillance’}

Another common concern is that a universal DNA database would subject innocents to lifelong ‘genetic surveillance’.\textsuperscript{54} Specifically, opponents argue that a universal database would limit our freedom to go embarrassing places,\textsuperscript{55} likely crime scenes,\textsuperscript{56} or protests\textsuperscript{57} for fear our presence or identity could be discovered through shed DNA. ‘Surveillance’ is a misnomer that should be avoided.\textsuperscript{58} Our DNA profiles would sit passively in a database, examined only by a computer program searching for matches to crime scene evidence.\textsuperscript{59} Nobody would (or could) conduct further tests on the destroyed DNA samples.\textsuperscript{60} Nor would our movements be tracked merely because we are in the database (as is everybody). Indeed, it would be both infeasible ‘to reconstruct a person’s travels by looking at DNA molecules’\textsuperscript{61} and unlikely to be attempted because far easier surveillance methods already exist. Unlike those surveillance methods, DNA profiles cannot reveal anything about a person’s movements, relationships, communications, or private characteristics.\textsuperscript{62} Thus, a DNA profile would only reveal a person’s movements if it matched a crime scene sample and law enforcement obtained a court order for the person’s name.

Rather than making everyone ‘an automatic suspect during his or her lifetime for any future crime’,\textsuperscript{63} a universal DNA database would instead promptly eliminate all but a handful of individuals as suspects for most crimes, protecting those eliminated from unnecessary, invasive police investigation.\textsuperscript{64} Additionally, our constitutional rights protect against a universal database being used to suppress dissent.

\begin{itemize}
\item See eg Kaye, supra note 40, at 79.
\item Such ‘familial searching’ occurs today because of current databases’ limited scope. Hence, a universal DNA database actually decreases the chance that private details about familial relationships will be exposed. See infra part IV-C.
\item Jules Epstein, ‘Genetic Surveillance’—The Bogeyman Response to Familial DNA Investigations, 2009 U. ILL. J. L. TECH. & POL’Y 141, 142 (2009).
\item Kaye & Smith, supra note 1, at 449.
\item Monteleoni, supra note 20, at 256.
\item Krimsky & Simoncelli, supra note 17, at 62–63.
\item Epstein, supra note 54, at 164.
\item Id.
\item Id.
\item Kaye & Smith, supra note 1, at 449.
\item Kaye, supra note 10, at 193.
\item Krimsky & Simoncelli, supra note 17, at 236.
\item Kaye & Smith, supra note 1, at 446. See also, infra part IV.C.
\end{itemize}
A universal DNA database does not subject us to ‘genetic surveillance’. Nor does it infringe our dignity or limit our autonomy. All a universal database prevents is the ability to hide one’s identity from the police—an ability ‘of little practical importance unless we want to commit crimes’.  

C. Database Security

Every electronic database comes with hacking concerns. For universal DNA databases, one raised hypothetical is hackers using the database to identify individuals in witness protection. Part II described various ways a universal database can be protected from hackers and designed to help ensure even hacked information is meaningless. This would especially be true in the hypothetical above if the database was not updated with the witness protection participant’s new name. Additionally, as was the case with other privacy concerns, hackers could more easily obtain the information they desire without hacking the database.

D. Framing Innocents

Skeptics also worry a universal DNA database would lead to more framing. Criminals have already begun planting DNA despite the lack of a universal database, however, to avoid prosecution and conviction. Moreover, several factors could help prevent successful framing attempts. Investigators can be trained to recognize planted DNA and find corroborating evidence before concluding the DNA’s source is the true suspect. Likewise, the requirement that prosecutors prove guilt beyond a reasonable doubt makes successful framing harder, especially if the true criminal also left identifiable DNA at the crime scene. ‘In any event, if the possibility of tampering with or misusing evidence were sufficient to deny its use, there is very little evidence that would ever be admissible’. Framing already occurs, both with DNA and otherwise, so concerns about framing do not justify withholding from law enforcement the gold standard of identification to assist in solving and preventing multitudes of crimes.

E. False Identification

Some opponents also worry that innocents could be falsely identified as suspects because of errors in the universal database, false matches, or misinterpretations of the implications of finding DNA at a crime scene.

Adopting universal standards for laboratories would help minimize the risk of erroneous profiles. And if an innocent is incorrectly identified due to an error, a new DNA sample can be obtained to correct the database and exonerate the falsely identified individual.

Similarly, if an innocent’s valid profile matches the CODIS loci of a crime scene sample, but the DNA found did not belong to the innocent, a new sample can be taken...
and examined beyond the CODIS loci, using strict privacy-protecting guidelines, to
demonstrate a false match. Such errors are unlikely to occur, however, because there is
only a one in one billion chance that ‘two unrelated individuals will have DNA profiles
that match at all thirteen loci’ and a universal database increases the confidence of
matches by ruling out a larger percentage of the population.

Finally, the worry that investigators and juries will take DNA evidence as virtually
conceivable of guilt, and thus ‘may not look for the real perpetrator or may
overlook other important evidence’, also exists for some non-DNA evidence and in-
dependent of a DNA database expansion. Regardless, the proper training of investi-
gators, a requirement for additional corroborating evidence to support an indictment,
and the reasonable doubt standard of proof can all help prevent an innocent from being
convicted based on the concerned false determination of guilt.

F. Putting the Privacy ‘Invasion’ in Context

Many people believe privacy no longer exists because we can be tracked by our phones
and online activity, sensitive information is hackable, and our lives are highly visible
through social media. In comparison, a universal DNA database that (a) contains only
one millionth of our DNA useful for identification only and (b) employs multiple pri-

IV. How Much Privacy Could You Gain?

Contrary to popular belief, a universal DNA database could actually increase privacy
by ending more intrusive investigative techniques, reducing crime, and decreasing false
convictions. This part will explain how ‘innocents are far more likely to be burdened by
suspicion and false accusation’—and privacy invasions—‘if we lack a comprehensive
DNA identification database than if we use one’.

A. Reducing Retrieval of ‘Abandoned’ DNA

DNA evidence is often unidentifiable because current databases contain profiles for
criminals only after they are caught. To help identify DNA, police retrieve ‘abandoned’
DNA of suspects through stalking and trickery because ‘we cannot refrain from leaving
our DNA everywhere we go’. Police will, for example, trick suspects into mailing a let-
ter to obtain DNA from the seal, or even more concerningly, will follow suspects until
they can obtain DNA from something the suspect has discarded. Both these methods
of retrieving abandoned DNA are legal, and neither requires a legal justification.

73 Dunstan H. Barnes, Big Brother is Watching You (And Your Family, Too): Familial DNA Searches in Criminal
Investigations, 50 No. 1 CRIM. L. BULLETIN ART 2 (Winter 2014).
74 KRIMSKY & SIMONCELLI, supra note 17, at 293.
75 Simoncelli, supra note 25, at 393.
76 Kaye & Smith, supra note 1, at 423.
77 KRIMSKY & SIMONCELLI, supra note 17, at 118.
78 Id. at 110.
79 Greg Miller, Familial DNA Testing Scores a Win in Serial Killer Case, 329 SCIENCE 262, 262 (2010).
80 See KRIMSKY & SIMONCELLI, supra note 17, at 116 (‘[N]o court has yet held police collection of ‘abandoned’
DNA illegal’).
81 Jho, supra note 41, at 880.
Such techniques are far greater invasions of privacy, and far closer to ‘surveillance’, than automatic computer searches of partial DNA profiles that, contrary to abandoned DNA, cannot be tested for sensitive information. Establishing a universal DNA database would protect individuals from these privacy intrusions by rendering the practice unnecessary.

B. Reducing Use of Electronic Medical Records as a De Facto Universal Database

Law enforcement also uses electronic medical records as a de facto universal database. For example, law enforcement caught a serial killer by obtaining his daughter’s Pap smear.82

Health care providers may legally disclose a broad array of basic demographic and health information to law enforcement, ‘including name, address, Social Security number, blood type, date of treatment, and a physical description’.83 Law enforcement can obtain even more information about a patient with a court order, grand jury subpoena, or an administrative request.84

Using medical records as a de facto universal DNA database provides law enforcement with far more sensitive information than CODIS markers would—sometimes about innocents under no suspicion. A carefully constructed universal DNA database would protect private medical information from such disclosure.

C. Reducing Invasiveness of Police Investigations

A universal DNA database can also reduce the invasiveness of investigations by ending the need for ‘dragnets’ and ‘familial searching’ to narrow suspect pools.

In a dragnet, police ask individuals in certain groups to provide ‘voluntary’ DNA samples to exclude themselves as suspects.85 Such dragnets are ‘highly inefficient’86 and ‘entirely ineffective’,87 but approached individuals are virtually required to submit to the dragnet’s hassle to avoid stigmatization.88

In ‘familial matching’, investigators look for a familial match in a DNA database to unidentified DNA evidence. This practice ‘cast[s] a cloud of suspicion over the entire family unit based on the criminality of one or more family members’,89 and causes innocents’ privacy to be invaded merely because of their believed familial connection to a suspect. The individuals investigated as a result may not even be related to the true suspect; ‘familial matching’ is based on ‘tenuous or tentative mathematical assumptions’.90 Familial searching also disproportionately invades the privacy of certain racial

---

82 Ellen Nakashima, From DNA of Family, a Tool to Make Arrests, WASHINGTON POST (Apr. 21, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/20/AR2008042002388.html.
83 KRIMSKY & SIMONCELLI, supra note 17, at 100; 45 C.F.R. § 164.512(f).
84 45 C.F.R. § 164.512(f).
85 See generally KRIMSKY & SIMONCELLI, supra note 17, at 46–63.
86 Id. at 62.
87 Id. at 62.
88 See Id. at 198.
89 Barnes, supra note 73.
90 KRIMSKY & SIMONCELLI, supra note 17, at 73.
and ethnic groups that are disproportionately represented in current databases, \footnote{Henry T. Greely et al, *Family Ties: The Use of DNA Offender Databases to Catch Offenders’ Kin*, 34 J. L. MED. & ETHICS 248, 259 (2006) (‘[M]ore than four times as much of the African-American population as the U.S. Caucasian population would be “under surveillance” as a result of family forensic DNA . . . ’).} ‘exacerbat[ing] disparities … that exist in the criminal justice system’. \footnote{KRIMSKY & SIMONCELLI, *supra* note 17, at 88.}

The invasiveness, ‘inconvenience, humiliation, and expense’ \footnote{Monteleoni, *supra* note 20, at 253.} of these techniques, and their racial implications, would disappear if a universal DNA database existed. \footnote{Greely, *supra* note 91, at 260.} Universal DNA databases are thus a ‘win-win situation’ \footnote{KRIMSKY & SIMONCELLI, *supra* note 17, at 276.} : law enforcement can more efficiently and accurately identify suspects, and innocents are protected from intrusive searches.

\section{D. Exonerating the Innocent}

A universal DNA database can reverse and prevent false convictions, along with the privacy, freedom, and dignity harms caused by false conviction. To the 350 innocents DNA evidence has already exonerated, \footnote{Innocence Project, *DNA Exonerations in the United States*, https://www.innocenceproject.org/dna-exonerations-in-the-united-states/ (accessed July 1, 2017).} ‘the value of a DNA database is beyond measure’. \footnote{Smith, *supra* note 26, at 385.}

\section{E. Deterring Crime}

Finally, a universal DNA database could increase safety and privacy by deterring crime. ‘DNA is five times as likely to result in identifying the suspect compared to finger-prints.’ \footnote{OFFICE FOR VICTIMS OF CRIME, *NATIONAL CRIME VICTIMS’ RIGHTS WEEK RESOURCE GUIDE: ENGAGING COMMUNITIES, EMPOWERING VICTIMS* 26 (2015), https://ovc.ncjrs.gov/ncvrw2015/pdf/FullGuide.pdf.} Increasing the chances criminals will be caught and punished deters \footnote{Cronin, *supra* note 8, at 150.} first-time crime and prevents serial crimes. Hence, a universal DNA database should be appealing even to those concerned about privacy invasions.

\section{CONCLUSION}

A properly constructed universal DNA database would pose only a minimal invasion of privacy. In return, it would decrease crime, reverse and prevent false conviction, make investigations more effective and efficient, and protect against far more invasive investigative techniques. A universal DNA database should be viewed as a way to protect ourselves and others, not as a ‘Big Brother’ invasion of privacy.