Reprinted from the

New York University
Annual Survey
of American Law

Shadow Dwellers: The Underregulated World of State and Local DNA Databases

Stephen Mercer & Jessica Gabel

Volume 69 Issue 3

2014

SHADOW DWELLERS: THE UNDERREGULATED WORLD OF STATE AND LOCAL DNA DATABASES

STEPHEN MERCER & JESSICA GABEL†*

* Chief Attorney, Forensics Division, Maryland Office of the Public Defender; Adjunct Professor of Law, University of the District of Columbia David A. Clarke School of Law. I owe a debt for the idea to closely examine the DNA collection, retention, and distribution practices of state and local law enforcement agencies to my professor, colleague, and father-in-law, Professor William G. McLain, III. In remarks before the U.S. House of Representatives, Rep. Alcee L. Hastings memorialized Professor McLain as:

> [A] champion for the powerless and a brilliant legal mind. . . . He worked tirelessly—often without compensation or recognition—on behalf of death row inmates and other criminal defendants who faced trumped up charges or other government abuses. He deplored racism and homophobia and provided legal counsel to those who were victimized by discrimination. Will was also a staunch advocate for the freedom of the press.

159 CONG. REC. E1345 (daily ed. Sept. 19, 2013) (statement of Rep. Alcee L. Hastings).

† Associate Professor of Law, Georgia State University College of Law. I would like to thank my fantastic research assistants Bryan Baird and Elizabeth Hornbrook for their dedicated work on this Article. I also owe a debt to the people who inspired me to delve deeper into issues that might otherwise get overlooked. My eternal thanks to Ryan Cino, Ursula Baird, Cory Gabel, and Trish Redmond.

INTRODUCTION

To do her part to help law enforcement, a Louisiana rape victim voluntarily provided her DNA so that her genetic information might help bring her attacker to justice.[1] After all, DNA saves lives and helps solve crimes.[2] Much to her horror, her DNA did not lead law enforcement to her rapist; rather, her DNA sample led to her brother's conviction for a separate string of crimes.[3] In Louisiana, DNA profiles from victims and suspects remain warehoused in local DNA databases indefinitely.[4] As a result, this woman essentially became a genetic informant on her brother. At arguably her most vulnerable point, this rape victim felt betrayed, because the police "did everything behind [her] back."[5] Her brother's attorney cautioned that "[s]uch cases might make rape victims think twice before reporting an attack."[6]

Louisiana's unexpected use of crime victim DNA and local DNA databases[7] to investigate crimes is not unique. This also occurs in Maryland, where police in Baltimore City and Prince George's County retain crime victim DNA in underregulated local DNA

1. *See* Ellen Nakashima, *From DNA of Family, a Tool to Make Arrests: Privacy Advocates Say the Emerging Practice Turns Relatives into Genetic Informants*, WASH. POST, Apr. 21, 2008, at A01.

2. *See* Jessica D. Gabel, *Indecent Exposure: Genes Are More than a Brand Name Label in the DNA Database Debate*, 42 U. BALT. L. REV. 561, 561 (2013); *see also* DNASAVES, http://dnasaves.org (last visited Oct. 6, 2014).

3. Nakashima, *supra* note 1.

4. *Id.*

5. *Id.*

6. *Id.*

7. For the purposes of this article, "databank" is used to refer to the repository of data at the national level of CODIS and "database" is used to refer to the state and local levels of CODIS.

databases from known persons that police cannot enter into the FBI's Combined Offender DNA Indexing System national DNA databank (CODIS).[8] These local police departments also maintain underregulated databases of DNA profiles from crime scenes that contain low-quality samples that are not permitted in CODIS.[9] Every week these local underregulated databases are compared to find complete or partial matches that link a known individual to crime scene evidence, or an unknown individual across multiple crime scenes[10]—with unintended consequences.

Louisiana and Maryland are not the exception, but rather the norm. The more than 190 public DNA laboratories that participate in the FBI's CODIS program also maintain databases at the state or local level[11] that may contain DNA from known persons or crime scenes that cannot be entered into the national databank.[12] The FBI closely regulates the categories of DNA profiles that can be entered into the national databank, but not the categories that partici-

8. *See, e.g.*, United States v. Davis, 657 F. Supp. 2d 630, 634–35 (D. Md. 2009) (describing unregulated operation of Prince George's County's local DNA database), *aff'd*, 690 F.3d 226 (4th Cir. 2012).

9. CECELIA CROUSE & D.H. KAYE, THE RETENTION AND SUBSEQUENT USE OF SUSPECT, ELIMINATION, AND VICTIM DNA SAMPLES OR RECORDS 2–5 (rev. ed. 2001) (discussing types of samples local and state databases contain).

10. *See* Brandon L. Garrett & Erin Murphy, *Too Much Information*, SLATE (Feb. 12, 2013, 8:22 AM), http://www.slate.com/articles/news_and_politics/jurisprudence/?2013/02/dna_collection_at_the_supreme_court_maryland_v_king.html.

11. *See CODIS and NDIS Factsheet*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Nov. 8, 2014). Although CODIS is used as a generic term to describe the network of police DNA databanks, it is actually software developed by the FBI for DNA laboratories to operate state and local DNA databases and to manage the DNA information they upload to the national DNA databank. *Id.*

12. While the FBI does not collect data from state and local laboratories that participate in CODIS regarding retention practices of "nonoffender samples," such as crime victim, elimination, or suspect samples that cannot be entered into the national databank, in 2000, the National Commission on the Future of DNA Evidence surveyed participating CODIS laboratories regarding current retention practices for nonoffender samples. Of the nineteen laboratories that responded, "[h]alf . . . determined that DNA profiles would be entered into [local] and [state] databases based on court opinions and 'analyst discretion' (defined as 'we import what we're comfortable importing')." CROUSE & KAYE, *supra* note 9, at 3. Seven laboratories did not have an internal CODIS manual with guidelines for analyst discretion. *Id.* Over two-thirds of the laboratories had no written definition of what samples constitute an elimination sample or a suspect sample. *Id.* Two of the laboratories entered a victim sample into the database if police notified the laboratory that the victim "is known to be associated with criminal activity." *Id.* These two laboratories also offered a quality assurance rationale to justify the inclusion of victims' samples. *Id.*

pating laboratories can store and search in databases at the local and state levels, creating a gap in regulation.[13]

Precisely because of this regulatory gap, police may expand underregulated local and state CODIS databases using DNA samples from crime victims, individuals who voluntarily provide elimination samples to aid an investigation, or samples collected from persons pursuant to a court order or warrant.[14] Police may also expand underregulated databases using crime scene DNA samples that do not meet the FBI's quality standards for inclusion in the national databank.[15]

This is the next wave of DNA database expansion. Unfortunately, it is accompanied by the perverse consequences that flow from allowing law enforcement to decide which citizens should be subjected to lifelong genetic surveillance in databases that are trawled for matches or partial matches to crime scene DNA samples rejected by the FBI. These consequences could very well endanger public confidence in the core mission of the regulated national DNA databank without any corresponding utility.

To better understand the current legal environment, Part I of this Article reviews the existing regulations and uses of DNA databases. From there, Part II addresses the current wave of expansion of underregulated state and local DNA databases. Turning to the root cause of some potential problems, Part III identifies the existing gaps in statutory and judicial regulation of law enforce-

13. The FBI specifically requires laboratories participating in CODIS to: (1) be an accredited laboratory; (2) have the status of a criminal justice agency; (3) have the status of a laboratory audited to FBI quality assurance standards; (4) comply with federal expungement law; (5) comply with federal law restricting access to information; and (6) limit demographic or criminal justice information directly linked to a profile. *See* FBI, NDIS Operational Procedures Manual § 2.1 (2014), *available at* http://static.fbi.gov/docs/NDIS-Procedures-Manual-Final-1-31-2013-1.pdf. The FBI does not require participating laboratories to ensure the categories of DNA profiles that may be stored and searched in state and local databases conform to the permissible categories of profiles in the national databank. *See id.* § 3.1. Also, the FBI does not require participating laboratories to adhere to the data standards for DNA profiles submitted to the national databank. *See id.* § 4.2.

14. *See supra* note 12 and accompanying text; *see also* Joseph Goldstein, *Police Agencies Are Assembling Records of DNA*, N.Y. Times, June 13, 2013, at A1.

15. *See* Crouse & Kaye, *supra* note 9. The FBI standards for data entered into the national databank require: (1) that crime scene samples be associated with a putative perpetrator; (2) limitations on mixtures of DNA; (3) a ban on low-template or low-copy-number profiles; and (4) the submitting laboratory to confirm that the data being submitted is sufficiently discriminating to result in only one match in the databank. FBI, NDIS Operational Procedures Manual, *supra* note 13, § 4.2.1.

ment agencies' DNA databases at the state and local level, with a particular focus on legal challenges to underregulated DNA databases in Maryland as a case example. Finally, the Conclusion identifies the objectives of regulation and makes specific proposals for legislatures to consider.

I.
EXISTING REGULATIONS AND USES OF DNA DATABASES

A. Background on Forensic DNA

Deoxyribonucleic acid (DNA) analysis is one of the most important advances in forensic science.[16] DNA testing provides police with an accurate and reliable method of comparing the DNA of a known person to DNA left at a crime scene by an unknown perpetrator.[17] The biological properties of DNA make it an ideal piece of evidence for police to focus on when investigating crime. Only a miniscule amount of biological material is needed to produce the DNA profile that law enforcement uses to compare crime scene DNA to DNA collected from a known person.[18] The crime scene DNA can be from different bodily fluids, such as blood, saliva, or semen, or any cell with a nucleus (including involuntarily shed skin cells) because an individual's entire DNA sequence can be found in the nucleus of any single cell.[19] Police can easily collect a DNA sample from a willing suspect with a cotton swab rubbed on the inside of the cheek,[20] and may also constitutionally collect DNA surreptitiously from involuntarily shed skin cells or other biological material.[21]

---

16. *See generally DNA Evidence Basics*, NAT'L INST. JUST., http://nij.gov/topics/forensics/evidence/dna/basics/Pages/welcome.aspx (last visited Nov. 8, 2014) (providing an overview of what sorts of DNA analyses are conducted in criminal cases and how those analyses are used).

17. *See* JOHN M. BUTLER, FORENSIC DNA TYPING: BIOLOGY, TECHNOLOGY, AND GENETICS OF STR MARKERS 1–2 (2d ed. 2005).

18. *See DNA Evidence: Basics of Identifying, Gathering and Transporting*, NAT'L INST. JUST., http://nij.gov/topics/forensics/evidence/dna/basics/Pages/identifying-to-transporting.aspx (last visited Nov. 8, 2014).

19. BUTLER, *supra* note 17, at 29.

20. *See DNA Buccal Collection Kit Training and Procedures*, FBI (Aug. 8, 2014), http://www.fbi.gov/about-us/lab/biometric-analysis/federal-dna-database/buccal-collection-kit-information. The collection of cheek cells from within the mouth cavity is referred to as a "buccal swab." *Id.*

21. *See, e.g.*, Raynor v. State, 99 A.3d 753, 755 (Md. 2014) (holding that a Fourth Amendment search did not occur when police collected and analyzed ge-

Because an individual's full DNA sequence is very large, CODIS utilizes a DNA profile that consists of only thirteen locations on certain chromosomes (13 CODIS Core Loci).[22] The 13 CODIS Core Loci provide for easy comparison of DNA profiles of known individuals to DNA profiles collected from crime scenes, helping to find matches that may identify the perpetrator of a crime.[23] A matching sequence of 13 CODIS Core Loci is ordinarily a rare enough event to uniquely identify a person as the source of DNA collected at a crime scene.[24] A perfect match between two complete profiles shows a common source.[25] A partial match, on the other hand, may identify a family member as the source of crime scene DNA because related persons inherit their DNA profiles from the same family tree.[26] A partial match may also happen by chance because low-quality crime scene profiles may not have sufficient information to reliably discriminate between persons who may be potential contributors.[27]

---

netic material from the armrest of a chair in which the defendant had been sitting during an interview).

22. BUTLER, *supra* note 17, at 94–97. This DNA profile is unique enough that when two of these DNA profiles are compared, "the average random match probability is rarer than one in a trillion unrelated individuals." *Id.*

23. *Id.* at 438. Police use of DNA is increasingly more sophisticated than just identifying suspects from visible stains of biological evidence like blood or semen found at crime scenes. Today, police are trained to collect biological evidence from a wide range of non-stained surfaces or articles that invisible cellular material may have been deposited on, such as doorknobs, steering wheels, hats, masks, or bandanas, to name a few. *See DNA Evidence: Basics of Identifying, Gathering and Transporting*, NAT'L INST. JUST., http://nij.gov/topics/forensics/evidence/dna/basics/Pages/identifying-to-transporting.aspx (last visited Nov. 8, 2014). Police are also trained to collect and use DNA for purposes beyond identification of a suspect. For example, DNA may change a defense in a rape case from alibi to consent by placing an individual at a location where he claims not to have been, or undermine a claim of self-defense by showing a suspect's DNA was collected from a weapon. *See id.*

24. *See* BUTLER, *supra* note 17, at 94–95. In the context of the federal DNA databank, "match" and "hit" are defined terms. A "match" occurs when a CODIS search results in an association between two or more DNA profiles, after which designated laboratory personnel from each affected laboratory start a process to confirm the match. *See* FBI, NDIS OPERATIONAL PROCEDURES MANUAL, *supra* note 13, § 6.1.1. A "hit" occurs when a confirmed or verified match aids one or more open investigations. *See id.* § 6.6.1.

25. Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248, 251 (2006).

26. *See* FBI, NDIS OPERATIONAL PROCEDURES MANUAL, *supra* note 13, app. G.

27. PETER GILL, MISLEADING DNA EVIDENCE: REASONS FOR MISCARRIAGES OF JUSTICE 125 (2014) ("Random match probabilities are more likely with low-template DNA profiles that are multi-contributor mixtures. False positives can occur as a result of 'composite results' from two or more contributors.") (citations omit-

In the 1980s, police began to use DNA to investigate unsolved cases in which biological evidence from a crime scene could be analyzed to develop a DNA profile, which could then be compared to DNA profiles collected from a group of possible suspects.[28] DNA was also used in cases where a suspect was known. The police could compare a known suspect's DNA profile to biological evidence found at the scene of a crime.[29] The potential value of databases of DNA from known individuals to provide investigative leads for unsolved crimes—as well as the substantial privacy concerns implicated when law enforcement collects, retains, and distributes DNA of known persons—was recognized early on.[30]

The first generation of forensic DNA testing, however, had practical limitations that checked the growth of DNA databases and limited their use to crimes where the DNA evidence was highly relevant to the identity of the perpetrator: early tests were expensive;[31] they required a blood sample from the suspect;[32] and, relative to

---

ted). In a mixed DNA profile of two or more persons, especially low-level mixtures of DNA, the "DNA data itself may demonstrate that different explanations are possible." Peter Gill et al., *DNA Commission of the International Society of Forensic Genetics: Recommendations on the Interpretation of Mixtures*, 160 Forensic Sci. Int'l 90, 100 (2006). For a plain-language explanation of the challenges of mixtures of low-quality DNA, see Norah Rudin & Keith Inman, *The Discomfort of Thought—A Discussion with John Butler*, CACNews, 1st Quarter 2012, at 8, 9–11.

The 2005–06 annual report for the United Kingdom's DNA databank further illustrates the problem of partial matches in a large database:

> Since May 2001, 182,612 crime scene profiles have been matched. A single suspect was reported for 132,178 of these match groups. A list of potential suspects was produced for the remainder. The identification of more than one potential suspect as the source of the DNA at some scenes is largely due to the significant proportion of crime scene sample profiles that are partial.

Nat'l DNA Database Strategy Bd., National DNA Database Annual Report 2005–2006, at 35 (2006) (U.K.), *available at* http://www.genewatch.org/uploads/?f03c6d66a9b354535738483c1c3d49e4/DNA_report2005_06.pdf.

28. Butler, *supra* note 17, at 2–4 (citing Joseph Wambaugh, The Blooding: The True Story of the Narborough Village Murders (1995)). Wambaugh tells the true story of an early use of DNA evidence: to solve the slayings of two teenage girls, the police in this case were the first to use Alec Jeffrey's discovery of a method to create a profile of the human genome with enough discrimination to exclude the entire target population of 4000 adult men as the source of semen at the crime scene except for the perpetrator of the crimes. *Id.* at 3.

29. *Id.*

30. *See, e.g.*, Nat'l Research Council, DNA Technology in Forensic Science 111, 113–16 (1992) (recognizing the value of DNA databases in investigating "crimes without suspects" as well as the potential for future misuse inherent in such databases).

31. Butler, *supra* note 17, at 325.

32. *See id.* at 4.

the subnanogram sensitivity of current technology, DNA profiles could only be developed from large amounts of biological evidence collected at a crime scene.[33] However, a visible amount of semen or blood meant certain identity evidence of the perpetrator.[34]

As awareness of the power of DNA grew, the increased demand for DNA analysis spurred the development of swifter, cheaper, and more sensitive tests.[35] The practical limitation of a blood draw as a means to collect a DNA sample from a person no longer exists; police can readily—and surreptitiously—collect a person's DNA sample from a discarded cigarette butt, chewing gum, saliva on a straw, or sweat on a chair.[36] Mass screenings of possible suspects can be accomplished with swabs of saliva.[37] A visible amount of a bodily fluid like semen, blood, or saliva at a crime scene is also no longer needed; police can collect and analyze trace amounts of "touch" DNA from surfaces like doorknobs, steering wheels, or windows.[38] "Touch" DNA is used in the prosecution of property crimes, drug offenses, and quality-of-life offenses like vandalism or trespass.[39] Unlike a visible amount of bodily fluid found at a crime scene, however, the relevance and reliability of low-level DNA profiles from surfaces likely to contain DNA from more than one person can be very uncertain.[40]

---

33. *See id.*

34. *See* GILL, MISLEADING DNA EVIDENCE: REASONS FOR MISCARRIAGES OF JUSTICE, *supra* note 27, at 14.

35. *Cf.* Peter Finn, *Revolution Underway in Use of DNA Profiles; Bid to Link U.S. Databanks Is Crime-Solving Edge*, WASH. POST, Nov. 16, 1997, at B04 (reporting on how new DNA technology was poised to expand DNA databases).

36. *Id.*

37. Jeffrey S. Grand, Note, *The Blooding of America: Privacy and the DNA Dragnet*, 23 CARDOZO L. REV. 2277, 2278 (2002). Grand also notes that in a mass-screening situation—also called a "DNA dragnet"—police often do not have probable cause to obtain a search warrant for any one individual in a group and thus need consent. *See id.* at 2295 & n.81. Usually, consenting to DNA testing excludes the target, but if any individual refuses, he comes under suspicion. *See id.* at 2284 & n.31, 2297 & n.95.

38. *See, e.g.*, Max Houck & Lucy Houck, *What Is Touch DNA?*, Scientific American (Aug. 8, 2008), http://www.scientificamerican.com/article/experts-touch-dna-jonbenet-ramsey/; *DNA Evidence: Basics of Identifying, Gathering and Transporting*, *supra* note 23.

39. *See* JOHN K. ROMAN ET AL., URBAN INST. JUST. POL'Y CTR., THE DNA FIELD EXPERIMENT: COST-EFFECTIVENESS ANALYSIS OF THE USE OF DNA IN HIGH-VOLUME CRIMES (2008), *available at* http://www.urban.org/UploadedPDF/?411697_dna_field_experiment.pdf; Nancy Ritter, *DNA Solves Property Crimes (But Are We Ready For That?)*, NAT'L INST. JUST. J., October 2009, at 2.

40. *See* sources cited *supra* note 27. The FBI bans low-level DNA profiles from the national databank, but not from state and local databases that participate in

This revolution in forensic DNA technology has created an opportunity for law enforcement to aggressively expand the collection and retention of DNA samples from known persons and crime scenes.[41] The first wave of expansion occurred at the national and state levels of CODIS: Congress and nearly every state relentlessly expanded the categories of convicted offenders and arrestees subject to mandatory DNA collection laws;[42] the courts routinely upheld these laws against challenges;[43] and powerful special interest groups advocated for mandatory DNA sampling from all convicted offenders and arrestees.[44]

The second-generation expansion of forensic DNA testing is now occurring largely under the radar at the state and local levels of CODIS. Precisely because federal law limits DNA profiles of known individuals in the national databank to persons who must

---

CODIS. *See* FBI, NDIS OPERATIONAL PROCEDURES MANUAL, *supra* note 13, § 4.2.1.10. The FBI also bans any partial or mixed profile that is likely to result in more than one match in the databank. *See id.* § 4.2.1.7.

41. *Cf. Rapid DNA or Rapid DNA Analysis*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/rapid-dna-analysis (last visited Nov. 9, 2014) (noting that the ongoing development of Rapid DNA technology will allow "automated extraction, amplification, separation, detection and allele calling without human intervention").

42. *See Forensic DNA Policy*, DNARESOURCE.COM, http://www.dnaresource.com/?policy.html (last visited Nov. 9, 2013). Twenty-eight states and the federal government now require DNA collection and analysis from at least some arrestees. *See* Maryland v. King, 133 S. Ct. 1958, 1968 (2013); Julie Samuels et al., *Collecting DNA from Arrestees: Implementation Lessons*, NAT'L INST. JUST. J., June 2012, at 19.

43. *See* Samuels, *supra* note 42; *see also, e.g.*, United States v. Kincade, 379 F.3d 813, 813 (9th Cir. 2004) (upholding the constitutionality of a federal statute authorizing the collection of DNA from certain federal offenders on parole, probation, or supervised release, absent individualized suspicion that the offenders had committed additional crimes); Green v. Berge, 354 F.3d 675 (7th Cir. 2004) (upholding the constitutionality of a Wisconsin statute authorizing the department of corrections to collect and store the DNA profiles of convicted felons); Groceman v. United States, 354 F.3d 411 (5th Cir. 2004) (upholding the constitutionality of a federal statute authorizing the collection of DNA from prisoners); United States v. Kimler, 335 F.3d 1132 (10th Cir. 2003) (holding the collection of a DNA profile pursuant to a federal DNA collection statute constituted a reasonable search and seizure under the "special needs exception" to the Fourth Amendment); Jones v. Murray, 962 F.2d 302 (4th Cir. 1992) (upholding the constitutionality of a Virginia statute authorizing the department of corrections to collect and store the DNA profiles of convicted felons); State v. Raines, 857 A.2d 19 (Md. 2004) (upholding the constitutionality of a Maryland statute authorizing the collection of DNA profiles of certain convicted persons).

44. *See, e.g.*, *About the DNA Resource Center*, NAT'L CTR. FOR VICTIMS OF CRIME, http://victimsofcrime.org/our-programs/dna-resource-center/about-the-dna-resource-center (last visited Nov. 9, 2014) (explaining the organization's commitment to increased use of DNA sampling from convicted offenders).

submit to DNA collection during a criminal prosecution,[45] police are exploiting the underregulated state and local levels of CODIS to retain DNA collected during investigations.[46] DNA profiles collected from a crime scene and analyzed during an investigation are called "casework" samples.[47] To be eligible for entry into the "forensic index" of the national databank, a casework sample must: (1) be reasonably probative of the identity of the perpetrator of a crime; (2) be not from a known person; and (3) not consist of complex mixtures or partial profiles that may hit to more than one person in

45. The Federal DNA Identification Act permits the FBI to operate a national databank to store and search DNA profiles collected from persons convicted of crimes, persons who have been charged in an indictment or information with a crime, persons detained under the authority of the United States, and relatives of missing persons who voluntarily provide a DNA sample in NDIS. 42 U.S.C. § 14132(a) (2012). The NDIS Operational Procedures Manual expressly bans the inclusion of victim DNA and DNA voluntarily submitted for elimination purposes in the national databank. FBI, NDIS Operational Procedures Manual, *supra* note 13, § 4.2.1.8. However, the Privacy Act Notice for the National DNA Index System suggests that the Department of Justice may have at one point considered retaining crime victim DNA to identify perpetrators of crimes who carried DNA of the victim away from the crime scene. 61 Fed. Reg. 37,495 (Jul. 18, 1996); FBI, NDIS Operational Procedures Manual, *supra* note 13, app. B (including in the "[c]ategories of individuals covered by [the National DNA Index System]: . . . Victims: Persons, living or dead, who have been victims of crimes where the perpetrator of the crime may have carried DNA of the victim away from the crime scene.").

46. *See* Goldstein, *supra* note 14. On a 2013 episode of National Public Radio's *Talk of the Nation*, a caller from Florida described an increasingly familiar scenario with casework samples:

> Yeah, I actually had exactly this experience that you were talking about. I have a small shop, and it was robbed in the night, and we called the police, and they came out and did the swabs, and they asked for samples from all of myself and my entire staff.
>
> They did not solve the crime . . . and they did not, in my opinion, fully explain that this DNA was going to go into a database for future use. And I feel like now, in effect, the police department, sheriff's department, has a, you know, a DNA of my entire staff. None of us are criminals. I don't think that they have a right to that information. I don't think they fully explained that we're going to keep this DNA and use it for future things.

Talk of the Nation: After SCOTUS DNA Ruling, What Changes for Police? (NPR radio broadcast June 17, 2013), *available at* http://www.npr.org/2013/06/17/192740045/after-scotus-dna-ruling-what-changes-for-police.

47. *See CODIS and NDIS Fact Sheet*, *supra* note 11 (describing "forensic (casework) DNA samples" as samples that are "attributed to the putative perpetrator" and collected from a crime scene as evidence, as opposed to samples taken directly from a suspect).

the databank.[48] These limitations do not exist at the state and local levels of CODIS.[49]

A regulatory gap allows state and local laboratories to collect, retain, and distribute their casework samples in the CODIS network at the state and local levels; federal law leaves to the states the regulation of these databases of DNA profiles that cannot be uploaded to the national databank.[50] All states mandate DNA collection from certain criminals, but only a few states regulate the collection, retention, or distribution of casework DNA samples.[51] The courts have similarly failed to develop new rules or faithfully apply existing rules to safeguard the privacy interests of persons who have volunteered their DNA to help police investigate a crime.[52] The result is that people who have not been convicted of a crime end up under lifelong genetic surveillance.[53]

New technology continues to expand the reach of underregulated databases. New advances, such as increases in the sensitivity of DNA testing, the lower cost of testing, simplified collection techniques, rapid results, and enhancements to the CODIS software create more opportunities for police to collect DNA from crime scenes and known individuals as a routine part of police work.[54] Increased

48. FBI, NDIS Operational Procedures Manual, *supra* note 13, §§ 4.2.1.7–4.2.1.8.

49. *Cf. id.* §§ 4, 6 (explaining that the FBI guidelines are statutorily authorized by Congress and apply to CODIS and the national databank).

50. *Cf.* 42 U.S.C. § 14132(b) (2012) (stating that the national databank can only contain samples that meet federal regulatory requirements); FBI, NDIS Operational Procedures Manual, *supra* note 13, §§ 4, 6.

51. Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 Wake Forest L. Rev. 767, 774–80 (1999).

52. *See, e.g.*, Varriale v. State, 96 A.3d 793 (Md. Ct. Spec. App. 2014) In *Varriale*, the defendant had "voluntarily provided DNA samples to the police in order to eliminate himself as a suspect in an alleged rape. Although the DNA sample cleared him of the alleged rape, it disclosed his involvement in an unrelated burglary that took place a few years earlier." *Id.* at 794–95. The defendant argued that his DNA profile should not have been retained in the state and local DNA databases once he had been "cleared of suspicion in the investigation in which the sample was obtained." *Id.* at 798. The court disagreed, and held that the Fourth Amendment does not regulate the retention of a DNA profile in a local CODIS database even when such retention exceeds the bounds of consent upon which the defendant agreed to have the sample removed from his body. *Id.* at 797–98.

53. *See id.*

54. *See* FBI, Codis: Combined DNA Index System (2010), *available at* http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-brochure-2010. The next generation of CODIS software will provide "enhanced kinship analysis tools" that will allow police to use CODIS databases—particularly at the state and local levels—to more effectively target family members of persons in the national databank. *Id.* at 1.

federal funding may encourage police to exploit these opportunities.[55] Accordingly, the number of profiles in underregulated state and local indices that cannot be uploaded to the national DNA databank is likely to continue to increase dramatically in the presence of lax database laws.

B. Federal Regulations

In 1990, the FBI launched a pilot piece of software to serve fourteen state and local DNA laboratories.[56] This software allowed police to generate investigative leads from biological evidence left at the scene of a crime.[57] The goal was to share DNA profile information in a databank described as a national DNA index system (NDIS).[58] Participating state and local laboratories could upload qualifying DNA profiles (also called DNA records) developed from crime scene evidence to the NDIS "forensic index" and DNA profiles of known individuals convicted of serious crimes to the NDIS "convicted offender" index.[59] This CODIS precursor searched for matches within the forensic index to identify crimes that might have been committed by a serial offender, as well as for matches between the forensic index and the convicted offender index to identify possible suspects.[60]

The software also provided participating local and state DNA laboratories with the ability to operate a local DNA index system (LDIS) and to share DNA profiles with other DNA laboratories in their state through a state DNA index system (SDIS).[61] The availability of the CODIS platform to retain and search DNA profiles provided local law enforcement laboratories the opportunity to compare DNA profiles from their casework that could not be

55. Over the past decade, the federal government has repeatedly increased funding to state and local laboratories to expand the reach of DNA collection and databases. In 2006, the federal government expanded the use of CODIS grants available for the creation of DNA profiles of arrested individuals. *See* DNA Fingerprint Act of 2005, Pub. L. No. 109-162, § 1003, 119 Stat. 3085 (codified as amended at 42 U.S.C. § 14135(a)(1) (2012)). In 2013, Congress enacted a law that provides funding for up to the entire first-year cost of implementing a DNA arrestee testing program. Katie Sepich Enhanced DNA Collection Act of 2012, 112 Pub. L. No. 112-253, § 3, 126 Stat. 2407, 2408 (codified at 42 U.S.C. § 14137a (2012)).

56. *CODIS and NDIS Fact Sheet*, *supra* note 11.

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. CROUSE & KAYE, *supra* note 9, at 3.

uploaded to the national DNA databank.[62] These databases may potentially include partial or mixed DNA profiles from crime scene evidence, of crime victims, of persons who voluntarily provided DNA samples to be eliminated from crime scene evidence, and of suspects who were not arrested or convicted.[63]

While CODIS was still in its pilot phase, the National Research Council published a seminal report on the use of DNA technology in the criminal justice system (NRC I).[64] NRC I presciently observed that "[i]f DNA profiles of samples from a population were stored in computer databanks (databases), DNA typing could be applied in crimes without suspects."[65] NRC I acknowledged the general similarity between a fingerprint databank and a DNA databank, but decisively rejected that analogy because "ordinary fingerprints and DNA profiles differ substantially in ways that bear on the creation and design of a national DNA profile databank."[66] NRC I explained:

> Confidentiality and security of DNA-related information are especially important and difficult issues, because we are in the midst of two extraordinary technological revolutions that show no signs of abating: in molecular biology, which is yielding an explosion of information about human genetics, and in computer technology, which is moving towards national and international networks connecting growing information resources.[67]

To address these concerns, NRC I recommended limiting the scope of who would be subject to DNA collection and avoiding testing genetic locations that are associated with traits and diseases.[68] NRC I also recommended maintaining identity information confidentially.[69] This would minimize the potential for misuse that could

62. *Cf. id.* at 2 (stating that while policies and procedures for including samples in the national databank are clear, policies and procedures for inclusion in state and local databases are much less clear).

63. *See id.*

64. *See* NAT'L RESEARCH COUNCIL, *supra* note 30.

65. *Id.* at 111.

66. *Id.* at 112–13.

67. *Id.* at 113–14.

68. *Id.* The 13 CODIS Core Loci are found on "non-coding" regions of an individual's chromosomes; that is, regions that do not store information that is used to make proteins. BUTLER, *supra* note 17, at 22, 94–97. The 13 CODIS Core Loci were selected to make up the standard CODIS DNA profile in the belief that they did not correspond to any particular traits or characteristics. *See* H.R. REP. NO. 106-900, pt. 1, at 27 (2000); BUTLER, *supra* note 17, at 22, 94, 443–44.

69. NAT'L RESEARCH COUNCIL, *supra* note 30, at 114–15.

occur if DNA identity information were linked to other databases that contain medical, criminal, social services, financial, or credit information.[70] It was precisely these privacy concerns that significantly influenced the earliest legislators authorizing the creation of a national DNA databank to include in the federal statute substantial restrictions on the collection, retention, and distribution of DNA and related information.[71]

Following the 1994 congressional authorization for a coordinated system of national, state, and local DNA databases, the FBI implemented the CODIS national DNA databank.[72] A relentless expansion of national, state, and local DNA databases quickly followed. By 1999, all fifty states required DNA collection and analysis from at least some convicted individuals.[73] In 2000, Congress followed suit and required DNA collection and analysis from individuals convicted of a limited set of federal offenses.[74] Congress extended that requirement in 2004 to all individuals convicted of federal felonies.[75] In 2004, Congress expressly permitted the FBI to accept into the national DNA databank DNA profiles of arrested individuals.[76] In 2005 and 2006, Congress extended federal DNA testing to all arrestees.[77] Similarly, today all fifty states require DNA collection from all individuals convicted of felonies, and twenty-eight states require DNA collection and analysis from at least some arrestees.[78]

---

70. *Id.*

71. *See, e.g.*, Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 210304(a)(1)–(3), 108 Stat. 2069 (codified as amended at 42 U.S.C. § 14132 (2012)).

72. *The FBI and DNA, Part 1—A Look at the Nationwide System that Helps Solve Crime*, FBI (Nov. 23, 2011), http://www.fbi.gov/news/stories/2011/november/?dna_112311.

73. *See* Hibbert, *supra* note 51.

74. *See* DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106-546, § 3(a)(1)–(2), 114 Stat. 2728 (codified as amended at 42 U.S.C. § 14135a(a)(1)–(2) (2012)).

75. *See* Debbie Smith Justice for All Act of 2004, Pub. L. No. 108-405, § 203, 118 Stat. 2269–71 (codified as amended at 42 U.S.C. § 14135a(d) (2012)).

76. *See* § 203, 118 Stat. at 2269–71.

77. *See* Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 155, 120 Stat. 587 (codified as amended at 42 U.S.C. § 14135a(a)(1)(A) (2012)); DNA Fingerprint Act of 2005, Pub. L. No. 109-162, § 1004, 119 Stat. 3085–86 (codified as amended at 42 U.S.C. § 14135a (2012)); 28 C.F.R. § 28.12 (2008).

78. *See* Hibbert, *supra* note 51; Samuels, *supra* note 42; *see also State DNA Database Laws—Qualifying Offenses*, DNARESOURCE (Sept. 2011), http://www.dnaresource.com/documents/statequalifyingoffenses2011.pdf.

In line with the expanding scope of persons subject to mandatory DNA collection, the number of laboratories using the CODIS software expanded to include over 190 state and local DNA databases.[79] Crime laboratories are also permitted to outsource DNA analysis to private companies that satisfy the FBI's quality assurance standards.[80] The combined effects of these expansions have caused the CODIS national DNA databank to grow exponentially: in 2000, there were about 400,000 offender profiles; by 2006, there were about four million offender profiles and 50,000 arrestee profiles.[81] According to the most recent available data, CODIS now contains over eleven million offender profiles and 1.9 million arrestee profiles.[82] The FBI claims to have produced over 219,700 hits assisting in more than 210,700 investigations, despite not tracking the number of convictions that are the result of a hit between DNA profiles from different crime scenes or a DNA profile from a crime scene and an offender profile.[83]

Nevertheless, the FBI is limited in what profiles it can include in the national databank.[84] NDIS can only include profiles authorized by statute.[85] Further, Congress expressly prohibited the FBI from including in NDIS any DNA samples that are voluntarily submitted for elimination purposes.[86] The FBI implemented additional quality standards that restrict the inclusion of profiles of known persons and from crime scenes.[87] The FBI does not allow state or local CODIS laboratories to upload enhanced DNA profiles created from very low-level amounts of human cells.[88] The concern is that part of the profile may be an artifact created during the testing process that enhanced testing techniques have amplified to seemingly detectable levels.[89] The imperative for reliable matches between DNA profiles in the national databank also means that the FBI limits state and local laboratories to uploading only profiles that are reasonably probative of the identity of a putative perpetra-

79. *See CODIS and NDIS Fact Sheet*, *supra* note 11.

80. *Id.*

81. *Id.*

82. *CODIS-NDIS Statistics*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics (last visited Sept. 7, 2014).

83. *See id.*

84. *See CODIS and NDIS Fact Sheet*, *supra* note 11.

85. *See supra* note 45.

86. *See id.*

87. FBI, NDIS Operational Procedures Manual, *supra* note 13, § 4.

88. *Id.* § 4.2.1.10.

89. *See id.*

tor.[90] Partial profiles and mixtures of DNA from crime scenes are also prohibited in the national databank unless the expected number of contributors to the mixture is fewer than the number of matches expected by chance from a search of the relentlessly expanding databank.[91]

C. State Regulation

States are responsible for developing their own regulations governing state and local DNA databases.[92] A minority of states regulate the categories of DNA profiles that can be stored and searched at the state or local levels. For example, Alaska permits only certain categories of DNA samples that cannot be uploaded to NDIS to be retained in the state database.[93] It also prohibits categories of samples from being entered in the state identification system that are not expressly permitted.[94] A local database practice that is in conflict with state law is preempted.[95] The only exemption to this regulation is that it must not prevent "a local law enforcement agency from performing DNA identification analysis in individual cases to assist law enforcement officials and prosecutors in the preparation and use of DNA evidence for presentation in court."[96]

By contrast, Michigan allows a suspect's DNA to be taken, but limits that "any other DNA identification profile obtained by the department shall not be permanently retained by the department

90. *See* 42 U.S.C. § 14132(a)(1)–(4) (2012); *see also* FBI, NDIS OPERATIONAL PROCEDURES MANUAL, *supra* note 13, §§ 4.2.1.8.

91. The FBI bans low-level DNA profiles from the national databank through its software licensing agreement with state and local CODIS laboratories. FBI, NDIS OPERATIONAL PROCEDURES MANUAL, *supra* note 13, § 4.2.1.10. The software agreement also includes the FBI ban on any partial or mixed profile that may result in more than one match in the databank. *Id.* at § 4.2.1.7.

92. *See supra* note 13 and accompanying text.

93. The Alaska statute allows the retention of DNA records from persons arrested or convicted in the state of a crime against a person or felony under certain statutes, certain minors adjudicated as delinquents, voluntary donors, certain persons required to register as sex offenders or child kidnappers, and anonymous donors for use in forensic validation, quality control, or population and statistical databases, as well as samples from crime scene evidence and unidentified human remains. ALASKA STAT. § 44.41.035(b) (2013).

94. *Id.* ("[S]amples not subject to testing . . . may not be entered into, or made a part of, the DNA identification registration system.").

95. *Id.* § 44.41.035(d)(3) (stating that local law enforcement may not establish or operate a DNA identification registration system unless the "procedure and rules for the collection, analysis, storage, expungement, and use of DNA identification data do not conflict with . . . [the] procedures and rules applicable to the [state] DNA identification registration system").

96. *Id.*

but shall be retained only as long as it is needed for a criminal investigation or criminal prosecution."[97] Vermont permits DNA profiles to be stored only at the state level and prohibits the entry into the state database of DNA "voluntarily submitted or obtained by the execution of a nontestimonial identification order . . . ."[98] Other states that subject local DNA databases to statutory requirements include Connecticut, Missouri, and Washington.[99] Yet other states appear to prohibit the use of local DNA databases altogether.[100]

The vast majority of states, however, do not curb or regulate the categories of DNA samples from known persons that may be stored in the state *or* local databases. These states allow the warehousing of far more DNA profiles and information than is allowed at the national level or by other states.[101] In the absence of affirmative statutory authorization for these local databases to contain DNA profiles that cannot be entered into the national databank, state law limiting the collection of DNA to qualifying offenders may implicitly prohibit the entry of such profiles.[102] Underregulated

97. MICH. COMP. LAWS § 28.176 (1990).

98. VT. STAT. ANN. tit. 20, § 1938 (1998).

99. CONN. GEN. STAT. § 54-102g (2012); MO. REV. STA. § 650.057 (2012); WASH. REV. CODE § 43.43.758 (2013).

100. *See, e.g.*, People v. Rodriguez, 764 N.Y.S.2d 305, 314–15 (Sup. Ct. 2003) (finding that because New York's expungement statute fails to mention local databases, local databases are improper).

101. *See, e.g.*, HAW. REV. STAT. § 844D-102(a) (2012) ("Nothing in this chapter shall be construed to restrict the authority of local law enforcement to maintain its own DNA-related databases or data banks."); IDAHO CODE ANN. § 19-5517 (2012) ("Nothing in this chapter shall limit or abrogate any existing authority of law enforcement officers to take, maintain, store and use DNA information or thumbprint impressions for law enforcement purposes."); LA. REV. STAT. ANN. § 15-620 (2012) ("Nothing in this Chapter shall limit or abrogate any existing authority of law enforcement officers to take, maintain, store, and utilize DNA samples for law enforcement purposes."); NEV. REV. STAT. § 176.0912(3)(a) (2012) ("An agency of criminal justice may establish procedures for . . . [r]etaining probative samples of biological evidence . . . ."); 44 PA. CONS. STAT. § 2336 (2013) ("Nothing in this chapter shall limit or abrogate any existing authority of law enforcement officers to take, maintain, store and utilize DNA samples for law enforcement purposes."). In Montana, when a suspect's profile is not allowed in the state DNA identification index, there is no regulation preventing the inclusion of a suspect profile in a separate suspect database by the crime lab. State v. Notti, 71 P.3d 1233, 1238 (Mont. 2003).

102. David M. Jaros, *Preempting the Police*, 55 B.C. L. REV. 1149, 1185–86 (2014) (suggesting that state courts take advantage of the intrastate preemption doctrine to ban certain law enforcement activities, such as the use of underregulated local DNA databases).

DNA databases may also violate state privacy law.[103] Further, the passage of state statutes to regulate the mandatory collection of DNA from convicted offenders and arrestees is a legislative recognition of the potential for misuse of DNA databases.[104] Nevertheless, state and local governments are empowered, subject to constitutional limitations, to authorize official police agencies to investigate and prevent crime to further the health, general welfare, and safety of the community, which may include the use of underregulated state or local DNA databases.[105]

D. Creatures of the Court

In *Maryland v. King*, the U.S. Supreme Court decided the Fourth Amendment reasonableness of a state law requiring the programmatic "collection and analysis" of DNA from persons charged with a crime of violence.[106] *King* considered the reasona-

---

103. For example, the Maryland Public Information Act limits categories of information that the state may retain:

> The State, a political subdivision, or a unit of the State or of a political subdivision may keep only the information about a person that: (1) is needed by the State, the political subdivision, or the unit to accomplish a governmental purpose that is authorized or required to be accomplished under: (i) a statute or other legislative mandate; (ii) an executive order of the Governor; (iii) an executive order of the chief executive of a local jurisdiction; or (iv) a judicial rule; and (2) is relevant to accomplishment of the purpose.

MD. CODE ANN., GEN. PROVISIONS § 4-102 (West 2014).

Further the act specifically addressed the collection of personal information by the government about its citizens:

> (1) Personal records may not be created unless the need for the information has been clearly established by the unit collecting the records. (2) Personal information collected for personal records: (i) shall be appropriate and relevant to the purposes for which it is collected; (ii) shall be accurate and current to the greatest extent practicable; and (iii) may not be obtained by fraudulent means.

Id. § 4-501. Finally, the act generally limits the information the state or a political subdivision can keep about a person to that information which is needed and relevant to accomplish a governmental purpose. *Id.* § 4-102. The obvious shortcoming to a claim under a state's public information law is the lack of a statutory suppression remedy.

104. *See supra* notes 93–100 and accompanying text.

105. *See* United States v. Kelly, 55 F.2d 67, 68 (2d Cir. 1932) (stating that law enforcement must be allowed to collect fingerprints of arrestees "for the good of the community," despite the "slight interference with the person involved in finger printing"); *cf.* Cady v. Dombrowski, 413 U.S. 433, 441 (1973) (recognizing that local police officers engage in "community caretaking functions, totally divorced from the detection, investigation, or acquisition of evidence relating to the violation of a criminal statute").

106. 133 S. Ct. 1958 (2013).

bleness of the collection, analysis, and retention of an arrestee's cheek cells to determine the arrestee's "DNA identification" for use in a closely regulated database to identify other crimes (unrelated to the crime of arrest) that the arrestee may have committed.[107] Because an arrestee's legitimate expectation of privacy is sharply reduced when he is being processed into state custody, *King* did not apply a per se Fourth Amendment analysis to a search for evidence of criminality.[108] Instead, to determine reasonableness, *King* balanced the governmental interest in an arrestee's DNA identification against an arrestee's legitimate expectations of privacy in his bodily integrity and DNA identification.[109] *King* explained that an arrestee's reduced expectation of privacy informed both sides of the balance: it both strengthened the governmental interest in DNA identification and reduced the arrestee's legitimate privacy expectations in the collection of his DNA and use of his DNA identification.[110]

King observed that, unlike an average citizen, an arrestee in the custody of the police is on notice that the government has a legitimate interest in his identity, including his DNA identification, which assists police in the administrative task of determining his criminal history.[111] The strength of the governmental interest follows directly from a person's volitional status:

> The legitimate government interest served by the Maryland DNA Collection Act is one that is well established: the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody. It is beyond dispute that "probable cause provides legal justification for arresting a person suspected of crime, and for a brief period of detention to take the administrative steps incident to arrest."[112]

King then balanced the strength of this governmental interest in an arrestee's DNA identification against the physical *and* informational privacy interests upon which DNA collection, retention,

---

107. *Id.* at 1967.

108. *Id.* at 1970. The "per se rule" requires that searches conducted outside the judicial process, without prior approval by a judge or magistrate, be considered presumptively unreasonable under the Fourth Amendment. *See, e.g.*, United States v. U.S. District Court (*Keith*), 407 U.S. 297, 317–18 (1972).

109. *King*, 133 S. Ct. at 1978.

110. *Id.*

111. *Id.* at 1971 ("When probable cause exists to remove an individual from the normal channels of society and hold him in legal custody, DNA identification plays a critical role in serving those interests.").

112. *Id.* at 1970 (internal quotation marks omitted).

and distribution intrude.[113] *King* concluded that the close statutory regulation of "DNA collection, retention, and distribution" eliminated the need for a warrant to check the power of the executive branch, and therefore held that the search was reasonable under the Fourth Amendment.[114] In these special circumstances, *King* concluded that "[t]he need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the 'interpo[lation of] a neutral magistrate between the citizen and the law enforcement officer.'"[115] *King* emphasized that "DNA collection is not subject to the judgment of officers whose perspective might be 'colored by their primary involvement in the often competitive enterprise of ferreting out crime.'"[116]

King did not directly address the collection, analysis, and retention of DNA samples from persons who have not been arrested for or convicted of a qualifying offense, leaving open the question of how the Fourth Amendment applies to crime victim, elimination, and suspect samples that have been volunteered to the police. *King* did confirm that a physical intrusion like a buccal swab rubbed against the inside of a cheek is a search under the Fourth Amendment.[117]

Because *King* considered the collection and use of an arrestee's DNA when considering the reasonableness of the search, one might presume that the Fourth Amendment applies to the use of DNA collected from persons with greater expectations of privacy than an arrestee or convicted offender. The privacy concerns for these individuals are amplified, because at each stage in the collection and use of volunteered DNA, a police officer must exercise his discretion without guidance from a generally applicable statute uniformly applied to all nonoffenders.[118] This fact distinguishes the rationales for the use of voluntarily obtained DNA from the administrative rationales of *King*. For nonoffender samples, there is no corresponding governmental interest to verifying the identity and criminal history of an arrestee being processed into state custody and considered for release pretrial. These factors demonstrate the need for a neutral and detached magistrate to determine whether

113. *Id.*

114. *Id.* at 1969–80.

115. Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (quoting Treasury Employees v. Von Raab, 489 U.S. 656, 667 (1989)).

116. *Id.* at 1970.

117. *Id.* at 1969.

118. Due to the fact that most federal and state DNA statutes do not regulate the collection or use of nonoffender samples. *See supra* Part I.B–C.

probable cause—a "time-tested means of effectuating Fourth Amendment rights"[119]—justifies the use of a crime victim, elimination, or suspect sample beyond the specific use for which it was volunteered.

Notwithstanding these different circumstances, some courts equate the scope of a person's consent to the removal of a DNA sample for use in one investigation to the scope of a search warrant for DNA.[120] These courts have held that once police have determined a person's DNA profile from a "lawfully" collected sample, the Fourth Amendment does not constrain the police from using the profile in future investigations.[121]

Subsequent to *King*, in *Varriale v. State*, Maryland's intermediate appellate court broadened the definition of a "lawfully" obtained DNA sample to include biological samples that police obtain with a consent form that limits use of the samples to a particular purpose.[122] The court in *Varriale* did not view the defendant's conditional consent to a bodily intrusion, or the police exceeding the bounds of consent, as limiting the "lawfulness" of the initial collection of biological samples.[123] Instead, the *Varriale* court read *King* as establishing that a reasonable person has no expectation of privacy

119. United States v. U.S. District Court (*Keith*), 407 U.S. 297, 317 (1972) (stating that the probable cause standard "accords with our basic constitutional doctrine that individual freedoms will best be preserved through [the] separation of powers").

120. *See, e.g.*, Pace v. State, 524 S.E.2d 490 (Ga. 1999). In *Pace*, the defendant signed a consent form for the collection of blood and hair from his body that stated those items would be used against him in a prosecution, and that he was a suspect in a particular murder; the defendant did not restrict his consent to the removal of his biological samples to that particular murder investigation. *Id.* at 497. Later, police used these samples to link the defendant to a second murder. *Id.* The Supreme Court of Georgia considered the subsequent use of the defendant's DNA profile to come within the scope of the consent given because the only remaining privacy interest was to not have one's DNA compared to crime scene evidence. *Id.* at 497–98. The court cited *Bickley v. State*, which held that police were not required to obtain a second search warrant to make subsequent use of a DNA profile initially obtained by a warrant in an earlier, unrelated investigation. *Id.* at 498 (citing Bickley v. State, 489 S.E.2d 167 (Ga. Ct. App. 1997)). *Bickley* explained that where police do not perform further testing beyond the scope of a search warrant, there is no search for Fourth Amendment purposes. *Bickley*, 489 S.E.2d at 170.

121. *See* Bickley, 489 S.E.2d at 170.

122. 96 A.3d 793, 797–98 (Md. Ct. Spec. App. 2014) (permitting a secondary investigative use of a DNA profile collected by consent from a person who limited the scope of its use to clearing himself of suspicion in an earlier investigation).

123. *Id.*

in his DNA identification.[124] Under this reading of *King*, police can use a consent form that limits the purpose for collecting biological samples to a particular investigation and then retain the resulting DNA profile in underregulated local and state databases for any future use. DNA identification becomes like a photograph or fingerprint of a person that police can use without Fourth Amendment constraint if the collection of the identification information is lawful.[125]

Varriale appears to be grounded on a misrepresentation of the common law doctrine of consent. Police do not "lawfully" obtain a person's DNA identification for any additional purpose when consent to the physical intrusion restricts the purpose of the search.[126] When police exceed the bounds of consent, the entry into the consenter's body becomes invalid, a common law concept akin to tres-

---

124. *Id.*

125. *See id.* at 797 (citing Wilson v. State, 752 A.2d 1250, 1272 (Md. Ct. Spec. App. 2000)) ("[T]he re-examination of the validly-obtained sample was no more of a search, for Fourth Amendment purposes, than is the reexamination of validly-obtained fingerprints."); *Wilson*, 752 A.2d at 1272 (holding that no Fourth Amendment search is implicated when police use DNA samples "lawfully obtained in the course of an earlier investigation . . . in the course of a new and unrelated investigation," and comparing lawfully obtained DNA samples to lawfully obtained "photographs, handwriting exemplars, ballistics tests, etc."); *cf.* Hayes v. Florida, 470 U.S. 811, 814 (1985) (stating that the fingerprinting process's lack of "repeated harassment" or "probing into private life" does not justify an unwarranted detention solely for the purpose of fingerprinting); Davis v. Mississippi, 394 U.S. 721, 723–28 (1969) (explaining that the Fourth Amendment prohibits the use in prosecution of fingerprints that were obtained during an unlawful detention). Courts that equate a DNA profile to fingerprints misapprehend two fundamental points: first, fingerprints impose the practical safeguard of a person *knowing* that police have collected his ten-print set of reference fingerprints; and second, unlike underregulated local and state DNA databases, national, state, and local fingerprint databases usually provide a procedure for a person to challenge the accuracy of the information stored in the database, and to seek expungement in appropriate circumstances. *See, e.g.*, 28 C.F.R. § 16.34 (2010) (detailing the procedure for an individual to change, correct, or update fingerprinting information retained by the FBI); MD. CODE REGS. 12.15.01.07 (2014) (giving an individual the right to inspect and challenge the completeness, content, accuracy, and dissemination of criminal history record information retained by state criminal justice agencies). Underregulated local and state DNA databases lack these minimal due process provisions, yet provide a much greater potential for future misuse. *See infra* Parts II-III.

126. *See* RESTATEMENT (SECOND) TORTS § 892A(3) (1979) ("Conditional consent or consent restricted as to time, area or in other respects is effective only within the limits of the condition or restriction."); *see also id.* § 168 ("A conditional or restricted consent to enter land creates a privilege to do so only insofar as the restriction is complied with."); *id.* § 168 cmt. b ("A consent to entry for a particular purpose confers no privilege to be on the land for any other purpose.").

pass or battery.[127] *Varriale*'s rationale illustrates how one court's view of the free-floating "expectation of privacy" test results in less personal security than the Fourth Amendment jurisprudence that is "tied to common-law trespass."[128] A decision that a person cannot limit the scope of consent to a bodily intrusion is consistent with one scholar's prediction that *King* will ultimately result in "less genetic privacy" by condoning a more "expansive use of DNA sampling."[129]

Before the explosion of DNA databases, however, some courts did recognize that a person could reasonably limit consent to a particular case. In *State v. Gerace*, a Georgia appellate court did not permit second uses of a DNA profile derived from a blood sample acquired by consent.[130] In that case, after a traffic accident, law enforcement read the defendant his implied consent rights and obtained consent to take a blood sample pursuant to state law, which allowed law enforcement to test for drugs and alcohol.[131] His blood sample was submitted for DNA testing, which led to his arrest for rape and aggravated sodomy.[132] The court recognized that "prior to receiving the DNA test results, [law enforcement] had no probable cause to arrest [the defendant] in connection with the rape."[133] Looking at the totality of the circumstances, however, the court held that "'[h]ad [the defendant] been cautioned that the results of the search and seizure of his blood would be used to supply evidence against him in an independent criminal prosecution, no consent might have been given.'"[134] The court declined to accept the state's proposal that, because the blood was obtained with consent, law enforcement was free to use it for any purpose.[135]

In a 1994 decision, the Oregon Court of Appeals read consent similarly. In *State v. Binner*, the defendant consented to having his

127. *See id.*

128. United States v. Jones, 132 S. Ct. 945, 949 (2012). *See also* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan J., concurring) (explaining the contours of the "expectation of privacy" test); *Varriale*, 96 A.3d at 796–98.

129. Elizabeth E. Joh, Term Paper, Maryland v. King*: Policing and Genetic Privacy*, 11 Ohio St. J. Crim. L. 281, 294 (2013).

130. 437 S.E.2d 862 (Ga. Ct. App. 1993).

131. *Id.* at 862–63.

132. *Id.* at 862.

133. *Id.*

134. *Id.* at 863 (quoting Beasley v. State, 419 S.E.2d 92, 94 (Ga. Ct. App. 1992)).

135. *Id.* at 862. This result was consistent with an earlier Georgia Supreme Court holding that evidence obtained by consent cannot be used for purposes beyond the scope of that consent. Turpin v. Helmeci, 518 S.E.2d 887, 889 (Ga. 1999).

blood taken for alcohol testing, which returned a result within the legal limit, but he declined to give a urine sample for drug testing.[136] Without a warrant, his blood sample was then tested for drugs, and came back positive.[137] The court determined that the defendant had a privacy interest in the contents of his blood and had expressly limited his consent to a test for alcohol.[138] Thus, by implication, he did not consent to the drug testing.[139]

In a 1970 decision, the Fifth Circuit also read consent similarly. *Graves v. Beto* was an appeal from a Texas District Court's grant of a writ of habeas corpus.[140] After the defendant's arrest for being drunk in public, police received a report of a rape, and the victim's description of her assailant resembled the defendant.[141] Some blood was found at the scene of the rape and the chief of police requested that the defendant consent to a blood draw.[142] In making the request, however, the chief represented that his purpose was solely to determine the alcohol content of the blood, and the defendant consented to the bodily intrusion for a sample of blood based on that limitation.[143] The defendant's sample was then analyzed for blood type and compared to the blood recovered at the rape crime scene—it matched.[144] The evidence, though, was held to be inadmissible because the consent was based on the chief's misrepresentations.[145] Therefore, the police had only limited authority to test for the presence of alcohol in the blood.[146]

Consent is a very powerful tool capable of relieving law enforcement officers of the burden of obtaining warrants and establishing probable cause.[147] The reasonableness of consent, however, is debatable considering the fundamentally coercive nature of many police encounters.[148] Perhaps the more difficult question is

136. 886 P.2d 1056, 1057 (Or. Ct. App. 1994).
137. *Id.*
138. *Id.* at 1059.
139. *Id.*
140. 424 F.2d 524 (5th Cir. 1970).
141. *Id.* at 524.
142. *Id.* at 525.
143. *Id.*
144. *Id.* at 524.
145. *Id.* at 526.
146. Graves v. Beto, 424 F.2d 524, 526 (5th Cir. 1970).
147. Fred W. Drobner, Comment, *DNA Dragnets: Constitutional Aspects of Mass DNA Identification Testing*, 28 CAP. U. L. REV. 479, 503 (2000).
148. *Id.* at 504–05 ("The flat statement by police that a sample would be collected could be considered a claim of lawful authority . . . which would obviate . . . putative consent. The police station setting itself, with large numbers of armed uniformed officers displaying indicia of authority, as well as the physical isolation

whether courts will properly apply a settled doctrine like the law of consent to a new technology that is perceived to be infallible.

E. Uncertainty in the Application of the Doctrine of Consent When Applied to DNA Collection

Traditionally, in the absence of a valid warrant the "[s]tate assumes the burden of overcoming the presumption of invalidity by demonstrating . . . that the warrantless search satisfied one of the firmly established exceptions to the warrant requirement."[149] When the government seeks to rely upon consent to justify the lawfulness of a search, it has the burden of proving that the consent was, in fact, freely and voluntarily given.[150] Because a person who consents to a search "may of course delimit as he chooses the scope of the search,"[151] the government must also prove that the search was within the actual scope of consent.[152] The allocation of the burden of proof means that "'*[w]here the evidence is inconclusive . . . the defendant wins*.'"[153]

In the context of DNA analysis, a court must decide between two basic consent scenarios: first, a nonoffender may have expressly consented to any future use of his DNA, or in the absence of express consent, the court may have determined that general consent to all future uses is implied;[154] and second, a nonoffender may have

---

experienced by the subjects, can also be considered a coercive environment where an individual does not feel free to refuse a request, whether reasonable or not.").

149. Graham v. State, 807 A.2d 75, 87 (Md. Ct. Spec. App. 2002); *see also* Jones v. United States, 357 U.S. 493, 500 (1958).

150. Bumper v. North Carolina, 391 U.S. 543, 548 (1968); *see also* United States v. Mendenhall, 446 U.S. 544, 557 (1980); Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973); Doering v. State, 545 A.2d 1281, 1290 (Md. 1988); Whitman v. State, 336 A.2d 515, 520 (Md. Ct. Spec. App. 1975).

151. Florida v. Jimeno, 500 U.S. 248, 252 (1991).

152. *Graham*, 807 A.2d at 88 (holding that a reviewing court must make its own de novo assessment of "1) the voluntariness of the ostensible consent and 2), even if voluntary, the actual scope of that consent").

153. *Id.* at 87 (quoting Duncan v. State, 340 A.2d 722, 725 (1975)).

154. *See Jimeno*, 500 U.S. at 252. The scope of consent—as it relates to genetic materials—plays an equally important role outside of the criminal justice system. One of the world's largest private DNA databases, Icelandic-based deCODE Genetics, Inc., wanted to use "genealogical records to estimate the genotypes of close relatives of its more than 120,000 research volunteers." *deCODE Denied*, GENOME WEB (June 21, 2013), http://www.genomeweb.com/blog/decode-denied. Iceland's Data Protection Authority required the company to obtain informed consent from all individuals whose genetic material would be used to conduct a genotype study of 280,000 living and dead relatives. Jocelyn Kaiser, *Agency Nixes deCODE's New Data Mining Plan*, 240 SCIENCE 1388, 1388 (2013). deCODE was founded in 1996 with the specific intention of establishing a "DNA database of the

expressly limited the scope of a consent search to a particular investigation or the court may imply such a limit from the circumstances. Under the traditional analysis, the government bears the burden of demonstrating either express consent, or that the use of the DNA was within the scope of implied consent as measured by the standard of objective reasonableness.[155] Objective reasonableness evaluates scope of consent as that which "an ordinary reasonable person would understand to be the scope of consent between the officer and the consenting person."[156]

The effectiveness of court regulation of local and state DNA databases is both uncertain and inconsistent, with perhaps too much focus on the particular facts of the instant case. For example, in *United States v. Kriesel*, a sharply divided panel of the Ninth Circuit addressed the government's interest in retention of a physical DNA sample.[157] After pleading guilty to a drug conspiracy charge, Edward Kriesel agreed to submit a blood sample for DNA analysis as a condition of his supervised release.[158] After his DNA profile was added to CODIS, Kriesel demanded the return of his actual blood sample, claiming the sample qualified as property.[159] The majority determined that although a blood sample qualifies as property, the government has a legitimate interest in retaining it.[160]

The Ninth Circuit aptly recognized that we live in a "rapidly changing world in which risks of undue intrusions on privacy are also changing."[161] The court stressed "that if scientific discoveries

whole Icelandic population and mining it for genetic markers linked to common diseases. The company never received legal approval for such a national database. But more than 140,000 volunteers agreed to allow the company to combine their medical and DNA information with Iceland's genealogy database." Jocelyn Kaiser, *Purchase by Amgen Won't Affect deCODE Genetics' Research, Founder Says*, SCIENCE MAGAZINE (Dec. 12, 2012, 5:05 PM), http://news.sciencemag.org/people-events/2012/12/purchase-amgen-wont-affect-decode-genetics-research-founder-says. After deCODE experienced significant financial difficulties, American company Amgen purchased deCODE with the intention of leading the industry in its ability to "identify and validate disease targets in human populations." Turna Ray, *With deCODE Purchase, Amgen Gains Genetics Expertise, Consumers Lose DTC Testing Option*, PHARMACOGENOMICS REPORTER (Dec. 12, 2012), http://www.genomeweb.com/clinical-genomics/decode-purchase-amgen-gains-genetics-expertise-consumers-lose-dtc-testing-option.

155. *See* State v. Binner, 886 P.2d 1056, 1059 (Or. 1994).

156. In re Tariq A-R-Y, 701 A.2d 691, 697 (Md. 1997) (Eldridge, J., dissenting) (citing Wilkerson v. State, 594 A.2d 597 (Md. Ct. Spec. App. 1991)).

157. 720 F.3d 1137 (9th Cir. 2013).

158. *Id.* at 1139.

159. *Id.* at 1142.

160. *Id.* at 1139–40.

161. *Id.* at 1147.

make clear that junk DNA reveals more about individuals than . . . previously understood, [the court] should reconsider the government's DNA collection programs."[162] It also noted that "[g]overnment and commercial entities enjoy increasing capacity to obtain, store, and analyze information about people, giving rise to increasing concerns about privacy."[163]

Recognizing that no single law enforcement investigation method is perfect—even one with "as good a record as CODIS"—the *Kriesel* dissent urged that investigative tools are "intended to aid in investigation, not to supplant it entirely."[164] The dissent strongly urged that "this case deal[t] not just with junk DNA or a CODIS profile derived from junk DNA, but the retention, for at least the remainder of an individual's lifetime, of his full genetic code."[165] In essence, the dissent urged that there is no justification for "the retention of the entirety of that individual's, and millions of others', private genetic information for the rest of their lives."[166] In opposition to the majority's dismissal of Kriesel's Fourth Amendment arguments, the dissent also observed, "We do not need scientists to discover anything new to know that a full specimen of an individual's DNA reveals private information about that individual's predisposition for certain diseases and disorders, paternity and other familial relationships, and racial ancestry."[167]

The *Kriesel* dissent underscores that the retention of a DNA profile and sample intrudes upon a privacy interest that extends beyond an interest in not getting caught. A "seized for one, seized for all" approach to volunteered DNA samples cannot be squared with the substantial privacy interests at stake. When police indefinitely retain consent samples in a database to search for evidence of criminality in unrelated cases, they must demonstrate that any con-

---

162. *Id.*

163. United States v. Kriesel, 720 F.3d 1137, 1139 (9th Cir. 2013). The dissent in *Kriesel* emphasized the distinction between the retention of the DNA sample and the retention of the DNA profile derived from it. *Id.* at 1150 (Reinhardt, J., dissenting).

164. *Id.* at 1156 (Reinhardt, J., dissenting) ("Our criminal justice system successfully deterred and punished crime for hundreds of years before the use of DNA evidence became standard practice.").

165. *Id.* at 1150.

166. *Id.* at 1153. The *Kriesel* dissent apparently understood CODIS to require expungement upon the death of the qualified convictee or arrestee. That is not necessarily the case. In Maryland, for example, expungement only occurs automatically if no conviction ever occurs, the conviction is reversed or vacated, or an unconditional pardon is granted. MD. CODE ANN., PUB. SAFETY § 2-511 (West 2009).

167. *Kriesel*, 720 F.3d at 1157 (Reinhardt, J., dissenting).

sent to the bodily intrusion was, in fact, freely and voluntarily given.[168] Because a person who consents to a search "may of course delimit as he chooses the scope of the search," the police must also prove that the search was within the actual scope of consent.[169] Does that mean the police must give advice to the target of a consent search that is in his best interest? The Supreme Court has clearly stated that police do not have to tell a person that he can decline to consent.[170]

At the same time, courts should not tolerate incomplete or garbled explanations in response to a nonoffender's questions about the implication of consenting to the collection of a DNA sample to aid in an investigation. Courts are unlikely to apply the principles of informed consent to DNA collection, although it remains the current standard of consent outside of the field of criminal justice.[171] As noted by the UK Human Genetics Commission, "'the difficulties involved in tracing and securing re-consent for different forms of medical research may make obtaining fresh consent impractical and would seriously limit the usefulness of large-scale population databases.'"[172] Genetic material used in medical research focuses on consent laws that "provid[e] research participants with relevant information in order to allow autonomous decision-making."[173] Failure to provide accurate and complete information to individuals violates the "ethical principles that underlie much consent jurisprudence."[174] Collecting and storing DNA samples en masse creates the possible threat of myriad "social and ethical concerns, including

168. Bumper v. North Carolina, 391 U.S. 543, 548 (1968); *see also* United States v. Mendenhall, 446 U.S. 544, 557 (1980); Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973).

169. Florida v. Jimeno, 500 U.S. 248, 252 (1991).

170. *Schneckloth*, 412 U.S. at 222.

171. Timothy Caulfield et al., *DNA Databanks and Consent: A Suggested Policy Option Involving an Authorization Model*, BMC MED. ETHICS, Jan 3, 2003, at 1. At the time of publication, only one state required informed consent for DNA samples volunteered to a statewide database. *See* ILL. ADMIN. CODE tit. 20, § 1285.40 (2012) ("Individuals may voluntarily provide samples for the Convicted Offender DNA database if they sign the informed consent section of the sample collection receipt contained in the collection kit, or by signing a separate consent form provided or approved by the Department of State Police. The voluntary sample will be used for criminal investigations by comparing the DNA profile from the individual with other DNA profiles in the database.").

172. Caulfield, *supra* note 171, at 2 (quoting HUMAN GENETICS COMM'N, INSIDE INFORMATION: BALANCING INTERESTS IN THE USE OF PERSONAL GENETIC DATA 94 (2002)).

173. *Id.*

174. *Id.*

possible genetic discrimination."[175] No reasonable person would consent to relinquishing his genetic material for any future use absent informed consent.

II.
SLEEPER CELLS: THE DEVELOPMENT OF LOCAL DNA DATABASES

In spite of the threat to individual privacy, law enforcement officials trumpet the value of local DNA databases as an effective crime-solving tool.[176] Local DNA databases "operate under their own rules," and as a result, they can catalogue a far greater number of DNA samples than their state and federal counterparts.[177] Laws regulating local DNA databases exist in a very small number of states.[178] Even among the limited laws regulating local DNA databases, there is "little consensus about what DNA retention policies are appropriate at the local level."[179] Without strict rules governing local DNA databases, local law enforcement agencies are able to exercise great discretion in the collection and use of DNA samples.[180] According to experts, with technological advances allowing for "rapid DNA testing," local DNA databases will continue to expand.[181]

A. "More is Better": Familial Searching and DNA Dragnets

The success of CODIS in generating investigatory leads from offender profiles stored in the national databank incentivizes police to expand state and local DNA databases to include more profiles.[182] Commentators have noted the opportunity for police to create "offline" DNA databases that are *not* connected to CODIS to target the "usual suspects" who are defined by demographics like race, class, and geographic location.[183] However, police are expanding state and local DNA databases that *are* connected to CODIS in ways that were probably never legislatively intended. Po-

175. *Id.* at 2–3.
176. *See, e.g.*, Goldstein, *supra* note 14.
177. *Id.*
178. *Id.* ("Alaska prohibits them. California and Hawaii are explicit in not precluding them. In many states, including New York, the law is silent on the issue.").
179. *Id.*
180. *See id.*
181. *Id.*
182. *See* Joh, *supra* note 129, at 287.
183. *E.g.*, *id.* at 286.

lice have discovered the backdoor to CODIS: federal law limits the DNA profiles that can be stored in the national databank, but these limits do not extend to state and local DNA databases.[184]

At the national level, DNA samples must adhere to federal requirements (including the offense and laboratory processing standards) before qualifying for inclusion in CODIS.[185] While many states have also adopted requisite standards for their own statewide DNA databases, some local police departments have established their own databases with little or no regulation.[186] In recent years, "a growing number of law enforcement agencies collect DNA for their own 'offline' databases."[187] Out of either frustration with the inefficiencies of state DNA laboratories or a desire to utilize DNA samples ineligible for collection under state or federal law, many local law enforcement agencies view local DNA databases "as valuable investigative tools."[188] Rather than limiting collection of DNA samples to convicted offenders and arrestees, many local law enforcement agencies also collect samples from "volunteers, victims, and suspects."[189] Innocent crime victims may "not necessarily realize their DNA will be saved for future searches."[190] Such collections are "profoundly disturbing" because DNA voluntarily given to the police to clear a name can be retained and used in the investigation of future crimes.[191]

Because of guidelines governing which samples are eligible for submission to the national databank, not all DNA profiles that are entered at the local and state levels will wind up being included at

184. *See* 42 U.S.C. § 14132(a) (2012) ("The Director of the Federal Bureau of Investigation may establish an index of—(1) DNA identification records of—(A) persons convicted of crimes; (B) persons who have been charged in an indictment or information with a crime; and (C) other persons whose DNA samples are collected under applicable legal authorities, provided that DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System; (2) analyses of DNA samples recovered from crime scenes; (3) analyses of DNA samples recovered from unidentified human remains; and (4) analyses of DNA samples voluntarily contributed from relatives of missing persons."); *see also supra* note 13 and accompanying text. Note that federal law firmly requires that "DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System." § 14132(a)(1)(C).

185. Joh, *supra* note 129, at 286.

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. Goldstein, *supra* note 14.

191. *Id.*

the national databank.[192] Local laboratories are free to decide what sorts of profiles can be stored only in the local database without running afoul of an inspection review, because these periodic inspections focus exclusively on samples that have been uploaded to the national databank.[193] In general, local databases warehouse two main types of samples: reference samples from known individuals and unknown crime scene samples.[194] While some local labs are proactive in their use of local databases, there are many that limit their own profiles to those that are permissible at the national level.[195] Those labs that are proactive in this regard—that is, those that include more legally obtained samples in the local database than may ultimately be submitted to the national databank—claim they are providing a more valuable service to their communities because they are likely to provide more investigative leads through CODIS.[196]

For example, during the course of the typical investigation, police will frequently collect many investigative reference samples.[197] Even if some of these samples are not eligible for entry into the national databank, some localities are allowed to keep the DNA profiles in their own local databases.[198] In addition, securing samples from otherwise ineligible defendants through plea bargains provides additional opportunities to solve crimes through CODIS.[199] Because criminals often commit crimes repeatedly in the same geographic area, local law enforcement is able to make the case for these local databases.[200] Little concern is expressed over the potential for gerrymandering the contours of a geographic area

192. Rockne Harmon, *The Power of LDIS*, Forensic Magazine (Apr. 16, 2013, 4:38 PM), http://www.forensicmag.com/articles/2013/04/power-ldis.

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.* CODIS has a 30% success rate, but forensic experts hypothesize that the use of local databases can "drive that success rate even higher" and "make our communities safer." *Id.*

197. *Id.*

198. Harmon, *supra* note 192.

199. *Id.*

200. *Id.* ("[D]ata released from the FBI indicates that in more than 87% of the offender hits in the database, the crime took place in the same state in which the offender provided a DNA sample. That follows the trend that police officers have seen for ages: criminals tend to offend locally, working the same area over and over—and, indeed, experience demonstrates that the offender may be convicted repeatedly in the same jurisdiction. Because of this behavior, having a geographically focused local database gives law enforcement agents an effective tool for solving crimes in their communities.").

to follow lines of race or class, the pooling of data between laboratories, the enhanced "CODIS-plus" profiles that include information necessary to identify a male's paternal line, or the cynicism of bartering for a young male's DNA that will permanently put him—and effectively his family—in a database with uncertain opportunities to expunge his genetic information.

Orange County, California, serves as a prime example of a city using a local DNA database on steroids. Law enforcement claims more is better, but is it? The Orange County local database has reached 80,000 offender profiles and shares information with neighboring jurisdictions.[201] Local officials tout a recently solved kidnapping and rape case from 2001 as an example of the database's effectiveness.[202] In 2012, a man was arrested for driving under the influence.[203] When his DNA sample was submitted to the local database following his conviction, it matched the DNA evidence collected from a 2001 crime scene, which was housed in the county lab.[204] Proponents, citing this example, argue that solving even one case justifies the expansion of underregulated local DNA databases at any cost.[205] But without greater transparency, it is not possible to determine whether data like this is being cherry picked. The lack of transparency in the demographics of the persons in the database and self-selected data about matches should make one skeptical of extraordinary claims of effectiveness.[206]

Underregulated DNA databases are also used to perform searches of familial DNA, a practice that the FBI does not routinely permit at the federal level.[207] In fact, a handful of states openly

---

201. *Id.*

202. *Id.*

203. *Id.*

204. Harmon, *supra* note 192.

205. *Cf. id.* ("'This is exactly the type of crime we were targeting when we created the Orange County District Attorney's local DNA database. I am confident that many violent, serious crimes such as this will be solved as more samples from local offenders are entered into the database,' said Tony Rackauckas, District Attorney, in a statement on behalf of Orange County.").

206. *See id.*

207. *See Familial Searching*, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/familial-searching (last visited Nov. 30, 2013) ("[F]amilial searching is not currently performed at the National DNA Index System."). "Familial searching" is a technique that relies on the similarities of DNA profile data between related persons to search for partial matches between crime scene evidence and profiles of known individuals in a database. *Id.* The partial matches may identify family members of the unknown individual from whom the reference DNA sample was collected at the crime scene. *Id.* In this way, the offender in the database functions as a "genetic beacon" that may point the way to family members as potential

practice familial DNA searches, while other states are silent or explicitly prohibit such use.[208] As of June 2011, California, Colorado, Texas, and Virginia are known to perform these familial searches.[209] Other states like Minnesota, Pennsylvania, and Tennessee have contemplated legislation pushing toward using familial DNA searches.[210] Whereas Maryland and the District of Columbia have explicitly prohibited such usage,[211] other jurisdictions have simply started employing familial searching based upon existing laboratory policies.[212] Local databases are a growing phenomenon, with little to no guidance and regulations as to search practices; local law enforcement agencies are governing themselves and creating in-house policies regarding DNA collection and sample usage.[213]

The scope of the problem is magnified when the casework of a local DNA laboratory intersects—as it often does—with DNA dragnets to identify the source of DNA collected at a crime scene.[214] When there is no hit of the unknown suspect profile to any offender profile in the national DNA databank, police may utilize a DNA dragnet—requesting DNA swabs from a target population that may largely be defined by economic class, race, or sex—to expand the collection of DNA to a selected group of individuals who are "associated" with the crime.[215] When these mass screenings of DNA sampling take place, typically the police have no particular-

---

suspects. Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN'S L.J. 3, 18 (2010).

208. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 Mich. L. Rev. 291, 302 (2010).

209. *Familial Searching*, *supra* note 207.

210. *Id.*

211. *Id.*

212. *Id.*

213. *See* Goldstein, *supra* note 14.

214. Phillip Pan, *Pr. George's Chief Has Used Serial Testing Before; Farrell Oversaw DNA Sampling of 2,300 in Fla.*, WASH. POST, Jan. 31, 1998, at B1 (reporting on new Prince George's County Police Chief's use of "serial DNA testing" in a high-profile rape and murder case).

215. *See* Richard Willing, *Privacy Issue Is the Catch for Police DNA 'Dragnets,'* USA TODAY, Sept. 16, 1998, at A1. The DNA samples are collected from the "group" en masse and without a warrant. *Id.* The first known DNA dragnet consisted of 4500 men in the English village of Narborough in 1986. Angus J. Dodson, Comment, *DNA "Line-Ups" Based on a Reasonable Suspicion Standard*, 71 U. COLO. L. REV. 221, 223–24 (2000). Furthermore, the term "associated" is often used very loosely. For example, in the Narborough dragnet, the men sampled were "associated" with a rape of two teenage girls simply because each subject lived in the same town as the victims. *See* Sepideh Esmaili, Note, *Searching for a Needle in a Haystack: The Constitutionality of Police DNA Dragnets*, 82 CHI.-KENT L. REV. 495, 499–500 (2007).

ized suspicion of any individual and focus the dragnet on those who may have had access to the crime scene, were in the vicinity, were of the same race as the perpetrator, or simply knew the victim.[216] In a dragnet situation, police lack probable cause to obtain a search warrant of any one individual in the group and therefore need consent to collect a DNA sample from the target.[217] Usually, individual targets in the group are excluded as suspects through DNA testing.[218] Conversely, when any individual target refuses consent, he comes under the heightened suspicion of police who may try to obtain a search warrant or surreptitiously collect a DNA sample.[219] And while these voluntarily submitted samples cannot be uploaded to the national DNA databank,[220] police maintain that they may upload the profiles into local and state DNA databases that participate in CODIS to search for evidence connecting the person to other crimes beyond the purview of the dragnet.[221]

A major concern is that the profiles of the individuals excluded as the source of any crime scene evidence may be permanently retained in the local and state databases because these casework profiles are treated as evidence.[222] A Louisiana case provides a

---

216. *See, e.g.*, Corbin v. State, 52 A.3d 946, 957 (Md. 2012) (stating that the police collected DNA samples from nine to twelve men who were deemed "associates of the victim"); *see also* Raynor v. State, 99 A.3d 753, 755 (Md. 2014) ("The victim contacted the police on numerous occasions throughout the next two years to inform them about potential suspects. During that time, the police obtained consensual DNA samples from approximately 20 individuals with possible connections to the 2006 rape, including several of the victim's neighbors. None of those DNA samples matched the DNA collected from the victim's home on the day of the rape.").

217. *See* Willing, *supra* note 215.

218. *See* Grand, *supra* note 37, at 2283–84.

219. *Id.* & n.31. Often, this is the goal of conducting the dragnet. *Id.* at 2278–79.

220. *See* FBI, NDIS Operational Procedures Manual, *supra* note 13, § 4.2.1. Although a DNA profile from a known person cannot be uploaded to the offender index unless collected pursuant to applicable state law, a state or local laboratory (like those in Maryland) that defines casework profiles from known persons as forensic samples may be able to exploit a regulatory exception that permits manual searches of forensic samples in the national DNA databank if exigent circumstances exist. *See id.* § 5.3.

221. *See* Grand, *supra* note 37, at 2279–80, 2283 & n.28.

222. Some courts have already refused to grant expungement requests from individuals who have been excluded as suspects in a criminal investigation. *See, e.g.*, Varriale v. State, 96 A.3d 793, 799 (Md. Ct. Spec. App. 2014) ("While it may seem anomalous that a volunteer like Varriale would have fewer statutory protections than someone who had been charged with or even convicted of a serious criminal offense, the anomaly is a result of the history and structure of the DNA Collection Act itself. When it was initially enacted in 1994, the Act authorized the collection,

prime example of the use of DNA dragnets and local DNA databases. Law enforcement in southern Louisiana launched an extensive manhunt for a serial killer who raped and murdered three women.[223] After recovering DNA evidence from the crime scenes, law enforcement attributed the murders to the same unknown male perpetrator.[224] In an effort to track down the killer, local and state law enforcement joined forces with the FBI to launch a task force "to generate leads on the serial killer's identity."[225] Two anonymous tips lead investigators to Shannon Kohler.[226] Although Kohler initially appeared willing to voluntarily provide law enforcement with a DNA sample, media reports caused him to refuse further cooperation.[227] Convinced of Kohler's involvement, law enforcement obtained a warrant and Kohler ultimately submitted to a cheek swab.[228] After law enforcement filed the warrant in the public records, local media quickly targeted Kohler "as a suspect in the serial killer investigation who was refusing to cooperate with police."[229] Kohler did not learn that his DNA was not a match to the killer until reading a local newspaper two months later.[230] After learning that he was no longer a suspect, Kohler requested the expungement of his DNA profile from "any place where it had been stored," including local databases.[231] The Fifth Circuit did not rule on whether Kohler's could seek expungement, and to date it is un-

---

retention, and (in some cases) expungement of DNA only from persons who had been convicted of felonies or of other enumerated crimes. In 2008, the General Assembly amended the Act to extend its provisions, including the expungement provisions, to persons who had been charged with a crime of violence, an attempt to commit a crime of violence, burglary, or an attempt to commit a burglary. The General Assembly, however, has yet to extend the expungement provisions to persons like Varriale, who voluntarily consent to the taking of a DNA sample.") (citations omitted); Amato v. Dist. Att'y for the Cape and Islands Dist., 952 N.E.2d 400, 410 (Mass. App. Ct. 2011) (holding that law enforcement's refusal to expunge an elimination profile in a database derived from a DNA sample voluntarily provided to police during a homicide investigation constitutes "unreasonable, substantial, and serious interference with privacy" under state statute restricting extraneous collection and storage of information by governmental units).

223. Kohler v. Englade, 470 F.3d 1104, 1106 (5th Cir. 2006).

224. *Id.*

225. *Id.* at 1107.

226. *Id.*

227. *Id.* For example, media reports indicated that the killer wore a size ten or eleven shoe, whereas Kohler told law enforcement he wore a size thirteen or fourteen shoe. *Id.*

228. *Id.*

229. Kohler v. Englade, 470 F.3d 1104, 1107 (5th Cir. 2006).

230. *Id.* at 1107–08.

231. *Id.* at 1108.

clear whether his DNA profile remains in a state or local database.[232]

B. "More is Better": Low Quality Crime Scene DNA

The underregulation of state and local DNA databases also means that low-quality DNA profiles developed from crime scene samples that cannot be uploaded to the national DNA databank are placed in state and local databases.[233] The risk of misidentification increases when degraded, partial, or irrelevant crime scene profiles are stored in databases.[234] DNA analysis of low amounts of DNA, called "low-copy number DNA," often fails to detect a complete profile and can add erroneous information.[235] In addition, state and local DNA databases are now being expanded to include other poor-quality DNA samples like "touch" DNA, driven by the increasing sensitivity of DNA analysis and an insatiable demand for DNA testing in a wide array of cases from property and drug crimes to quality-of-life offenses.[236]

---

232. Although the *Kohler* decision did not resolve Kohler's request for expungement, it does emphasize the need for thorough judicial scrutiny of decisions to obtain DNA samples from those suspected of, but not convicted of, committing a serious crime, and the constitutional requirement that these decisions satisfy the probable cause standard. *See id.* at 1109–12. *Kohler* also recognized that the intrusiveness of the search extends beyond the collection of a saliva sample to include an assessment of the analysis and storage of the sample. *Id.* at 1109 n.4 (noting that for Fourth Amendment purposes, a chemical analysis of lawfully obtained blood, breath, and urine samples, as well as the collection, analysis and storage of blood and saliva, constitutes a search).

233. *See, e.g.*, William C. Thompson, *Forensic DNA Evidence: The Myth of Infallibility*, *in* GENETIC EXPLANATIONS: SENSE AND NONSENSE 227 (Sheldon Krimsky & Jeremy Gruber, eds., 2012), *available at* http://ssrn.com/abstract=2214379.

234. *See* BUTLER, *supra* note 17, at 526; GILL, *supra* note 27, at 125 ("Random match probabilities are more likely with low-template DNA profiles that are multi-contributor mixes.").

235. *See* Peter Gill, *Application of Low Copy Number DNA Profiling*, 42 Croatian Med. J. 229 (2001); Carole McCartney, *LCD DNA: Proof Beyond Reasonable Doubt?*, 9 NATURE REVIEWS GENETICS 325 (May 2008).

236. *See* Thompson, *supra* note 233, at 232 (discussing how a "touch" DNA sample in a DNA database falsely implicated a California man in a rape case); *see also* John Butler, Nat'l Inst. of Standards & Tech., Presentation at the National Institute of Justice Conference: What We Have Learned (June 20, 2012), *available at* http://www.cstl.nist.gov/div831/strbase/mixture/NIJ2012-WhatLearned-Butler.pdf (recognizing the variation in how analysts in crime laboratories interpret complex mixtures); Charlotte J. Word, *Mixture Interpretation: Why Is It Sometimes So Hard?*, PROMEGA (2011), http://www.promega.com/resources/profiles-in-dna/2011/mixture-interpretation-why-is-it-sometimes-so-hard/ (explaining the challenges of interpreting multi-source DNA mixtures).

The number of partial crime scene profiles that matched multiple persons in Great Britian's national DNA databank illustrates the scope of the concern. Between May 2001 and September 2006, 182,612 crime scene profiles were matched.[237] A single suspect was reported for 132,178 of these match groups; for the remainder of matches (nearly 50,000), a list of potential suspects was produced.[238] In its annual report, the agency overseeing the database explained that "[t]he identification of more than one potential suspect as the source of the DNA at some scenes is largely due to the significant proportion of crime scene sample profiles that are partial."[239]

The existence of a database that contains low-quality DNA profiles developed from crime scene samples means that individuals whose profiles are contained in the database, and their family members, may be falsely connected to criminal investigations.[240] Whereas FBI regulations exclude these poor-quality samples from the U.S. national databank in an attempt to ensure the quality of investigative leads generated from a "hit" to an individual in the convicted offender or arrestee indices, many state and local

237. NAT'L DNA DATABASE STRATEGY BD., *supra* note 27.

238. *Id.*

239. *Id.*

240. *See* Thompson, *supra* note 233, at 232; SHELDON KRIMSKY & TANIA SIMONCELLI, GENETIC JUSTICE: DNA DATA BANKS, CRIMINAL INVESTIGATIONS AND CIVIL LIBERTIES 300–04 (2011) (discussing the myth of objectivity in DNA interpretation and the myth that a mismatch between DNA profiles excludes a person from suspicion). For example, in a Sacramento, California rape case, a DNA analyst tested a swab of the victim's breast and identified a male DNA profile. *See* M.S. Enkoji, *DNA Lapse Puts Scrutiny on Lab Work*, SACRAMENTO BEE, Sept. 14, 2006, at B1. The profile did not meet the criteria for upload to the national DNA databank, but was included in the state DNA database. *Id.* It hit to the profile of a man who lived in the Sacramento area. *Id.* However, a subsequent police investigation cast doubt on the man's involvement in the crime. *Id.* A supervisor in the crime laboratory checked the analyst's interpretation and discovered the analyst made an incorrect assumption about the number of male contributors to the low level mixture of DNA recovered from the victim's breast swab that caused the false hit. *Id.*

Another recent example of low-level mixtures of recovered DNA comes from the highly publicized Amanda Knox trial. Renowned forensic expert Greg Hampikian of Boise State University has advocated for Knox's innocence based on DNA evidence. Eulonda Sklyes, *The Role of Alleged Trade Secret Forensic Evidence in the Amanda Knox Murder Case*, ORRICK TRADE SECRETS WATCH BLOG (Nov. 8, 2013), http://blogs.orrick.com/trade-secrets-watch/2013/11/08/the-role-of-alleged-trade-secret-forensic-evidence-in-the-amanda-knox-murder-case/. He claims the DNA evidence used at trial was contaminated through the "'casual transfer' of DNA evidence from one object to another." *Id.* The details of Hampikian's specific arguments remain unknown based on Boise State University's allegations that his arguments and research are protected trade secrets. *Id.*

databases may include them.[241] Furthermore, while the FBI audits the profiles that local and state laboratories upload to the national databank to further ensure the quality of its investigative leads and ensure compliance with its upload standards, these audits do not extend to profiles contained in the local and state laboratories.[242]

When there is uncertainty about the number of contributors to a crime scene DNA sample and whether all of the data is complete, a forensic analyst's interpretation of the data to identify profiles of the contributors becomes prone to subjective assessments, bias, and error. In a 2011 study, seventeen qualified DNA analysts from accredited crime laboratories were asked to evaluate DNA data that had actually been used to prove a Georgia man guilty of participating in a gang rape.[243] The analysts were provided with the scientific data necessary to interpret the results, but they were not provided with any contextual information about the facts of the case.[244] Twelve of the analysts concluded that the DNA profile of the Georgia man excluded him as a possible contributor, four found the data to be uninterpretable, and only one found that he was a contributor to the forensic mixture of DNA.[245] The wide variation of results "demonstrates that DNA mixture interpretation has subjective elements and may be susceptible to bias and other contextual influences."[246]

C. "More is Better": Turning to the Private Sector

The lack of effective regulation for CODIS-affiliated local DNA databases also encourages police to obtain DNA database software in the private market. The Local DNA Index System (LODIS) is one example of such software. It functions "to bring forensic DNA technology down to the average city or county level."[247] The Palm

241. FBI, NDIS Operational Procedures Manual, *supra* note 13, § 4.2.1.3; *see also supra* note 9 and accompanying text.

242. *See* FBI, The FBI Quality Assurance Standards Audit for Forensic DNA Laboratories (2011), *available at* http://www.ncdoj.gov/getdoc/95b5346d-dfa0-4bca-b423-1e186811895e/2012-NC-DNA-Database-Audit.aspx (describing the scope of the audits as the scope necessary to establish quality assurance requirements for samples included in CODIS).

243. Itiel E. Dror & Greg Hampikian, *Subjectivity and Bias in Forensic DNA Mixture Interpretation*, 51 Sci. & Just. 204, 205 (2011).

244. *Id.*

245. *Id.*

246. *Id.*

247. Bill Berger et al., *LODIS, A New Investigative Tool: DNA is Not Just Court Evidence Anymore*, The Police Chief (April 2008), http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1465&issue_id=42008.

Bay Police Department in Florida deployed LODIS in three separate phases.[248] The first phase, completed in November 2007, "had as its primary goal the training of patrol officers in DNA collection."[249] Police officers were "encouraged to collect samples at all crime scenes."[250] The second phase of the project allowed officers to "review DNA test results from a car computer over an encrypted, secure network."[251] Phase three culminated in the analysis of the "overall results in impact on crime" in order to "determine if the process is affordable for the average agency."[252]

"LODIS was designed specifically to provide local agencies with a system to create local DNA databases, which are flexible to meet the unique investigative needs of local law enforcement agencies."[253] Ultimately, local agencies benefit from LODIS by being able to "deploy CODIS at their agencies [ ] to be used in conjunction with other investigative techniques on more commonly committed crimes."[254] "As such, it provides an approach for implementing the local DNA index system (LDIS) component of CODIS on a broad scale and independent of any limitations in DNA testing capacity at the state laboratory level."[255]

D. Maryland as a Case Example

Maryland is home to two separate levels of underregulated DNA databases. First, each of the five local police agencies in the state maintains its own underregulated database.[256] These local police agencies operate DNA laboratories and upload profiles to CODIS.[257] Each LDIS retains DNA samples from known individuals that are not eligible to be uploaded to the state or national DNA

248. *Id.*

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

253. Berger et al., *supra* note 247.

254. *Id.*

255. *Id.*

256. *See History of Maryland's DNA Database*, MD. GOVERNOR'S OFF. CRIME CONTROL & PREVENTION, http://www.goccp.maryland.gov/dna/maryland-database.php (last visited Dc. 3, 2014); *see also* DEP'T OF MD. STATE POLICE, 2011 ANNUAL REPORT: MARYLAND STATE POLICE FORENSIC SCIENCES DIVISION STATEWIDE DNA DATABASE REPORT (2012). Those agencies are the police departments in Montgomery County, Prince George's County, Baltimore County, Baltimore City, and Anne Arundel County. *Id.*

257. *Id.*

databank.[258] The second level involves the "suspect" index within the Maryland State DNA database. The suspect index includes DNA samples collected pursuant to a search warrant from known individuals who are not already catalogued as arrestees or convicted offenders.[259] These suspect samples are not eligible for inclusion in the national DNA databank.[260] The suspect index also includes DNA samples collected from any individual that the police, at one time, labeled a "suspect"—even if the DNA evidence cleared the person of suspicion.[261] The Maryland DNA Databank Act does not authorize the "suspect" index and the Maryland State Police have issued no governing regulations, other than to define suspect DNA as crime scene DNA.[262] Casework evidence samples are also included within the definition of crime scene evidence.[263]

By defining the suspect index and casework evidence samples as crime scene evidence, the genetic privacy of crime victims, individuals who volunteer DNA samples to aid an investigation, and persons who provide a DNA sample to clear themselves of any suspicions—whether by consent or pursuant to a warrant—is intruded upon to a far greater degree than the privacy interest of convicted offenders and persons arrested for serious crimes; even convicted offenders and persons arrested for serious crimes are able to enjoy the statutory protections contained within the Maryland DNA Collection Act.[264] Important safeguards provided by the Maryland DNA Collection Act include:

---

258. *See, e.g.*, Varriale v. State, 96 A.3d 793, 795–96 (Md. Ct. Spec. App. 2014) (recounting how Varriale had been cleared of suspicion by the Anne Arundel County Police Department during a prior investigation in which his DNA had been sampled, but that his DNA profile was uploaded into the "suspect index" anyway); *supra* note 8 and accompanying text.

259. *See id.*

260. *See supra* note 15 and accompanying text.

261. *See supra* note 258.

262. *See* MD. CODE REGS. 29.05.01.01(B)(17) (2012). In 2011, the Maryland Department of State Police submitted 1901 crime scene DNA evidence samples that "qualified for inclusion . . . in the Statewide DNA database." OFF. OF LEG. AUDITS, MD. GEN. ASSEMB., CRIME SCENE DNA COLLECTION AND ANALYSIS REPORTING BY LAW ENFORCEMENT AGENCIES 2 (2013).

263. *See* MD. CODE ANN., PUB. SAFETY § 2-501(i)(3) (West 2013); MD. CODE REGS. 29.05.01.01(B)(17) (2014). DNA samples collected from persons other than qualifying convictees or offenders—that is, persons who have *not* been arrested—are treated as a "forensic or evidence sample." MD. CODE REGS. 29.05.01.01(B)(17) (2014). A "forensic or evidence sample" means DNA obtained "from an item of evidence *or an individual, including suspect samples*, other than one required to be collected pursuant to [MD. CODE ANN., PUB. SAFETY § 2-501 *et seq.*]." *Id.* (emphasis added). For Maryland's definition of "DNA Sample," see § 2-501(i).

264. *See* §§ 2-501 to 2-514.

- Limitations on whose profiles are to be included in the database;[265]
- Restrictions on the use of DNA samples included in the database;[266]
- Limitations on whether the state DNA database may be used to conduct familial searches;[267]
- Reporting requirements to the legislature regarding the utility of the database and the racial demographics of the persons in the database;[268] and

---

265. *Id.* In 1994, when the Maryland General Assembly established a state database of DNA profiles, it required DNA collection and analysis from individuals convicted of rape and other sexual offenses. *See* 1994 Md. Laws 2187. In 1999 and 2002, the General Assembly expanded the Act to cover individuals convicted of all felonies and some misdemeanors. *See* 2002 Md. Laws 3716; 1999 Md. Laws 2997. In 2008, the General Assembly temporarily expanded the Act to cover individuals who had been charged with, but not yet convicted of, crimes of violence and burglaries. § 2-504(a)(3); 2008 Md. Laws 3232. Under the current version of the Act, the collection of DNA samples from covered individuals is mandatory; with regard to individuals who have been charged but not convicted, the Act provides that the state is to collect the sample at the time of the charge. § 2-504(b)(1). In 2013, the General Assembly removed the Act's sunset provision. *See* H.B. 292, 433rd Gen. Assemb., Reg. Sess. (Md. 2013).

266. § 2-505(b)(2). The Act further provides that, "[t]o the extent fiscal resources are available," DNA samples "shall be . . . tested" for several purposes, including "as part of an official investigation into a crime," "to analyze and type the genetic markers contained in or derived from the [samples]," and "for research and administrative purposes," such as "develop[ing] a population database after personal identifying information is removed" and "support[ing] identification research and protocol development of forensic DNA analysis methods." *Id.* § 2-505(a). In aid of those purposes, the Act specifically authorizes the state to prepare and store "DNA records" (the Act's term for DNA profiles), which can be compared with similar profiles in national and state databases. *Id.* §§ 2-502(d), 2-504(d)(1), 2-505(b), 2-506(a).

267. *Id.* § 2-506(d) (prohibiting familial searches of the state DNA database). The Director of the statewide DNA database has expressly limited the ban on familial searching to DNA samples from arrestee and convicted offenders: "The Statewide DNA Data Base System may not be used for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the *DNA arrestee or convicted offender* sample was acquired." MD. CODE. REGS. 29.05.01.06(B) (2014) (emphasis added).

268. § 2-513. The reporting requirement is intended to gather data on whether the disproportionate representation of African Americans in the criminal justice system translates into African Americans also being disproportionately represented in governmental DNA databases. *See* § 2-513(b)(3); MD. GEN. ASSEMB. DEP'T OF LEGAL SERVS., THE 90 DAY REPORT: A REVIEW OF THE 2008 LEGISLATIVE SESSION, Gen. Assemb. 425, 2008 Sess., at E-14 (2008). In the first three years since Maryland has begun collecting data about racial demographics of arrestees from whom DNA samples were seized, minorities have consistently represented approximately 60% of the total number of individuals subject to the compelled collection

- Most importantly, expungement provisions.[269]

As discussed in Part III, the underregulated local and state indices in Maryland represent a substantial privacy intrusion upon individuals who have not (1) engaged in conduct that lessens their expectation of privacy, or (2) consented to the indefinite retention of their DNA in a law enforcement database that does not even offer the protections afforded convicted offenders or arrestees.

Although many states are following the Maryland trend, some jurisdictions are taking a closer look at the local use of DNA databases in response to *King*.[270] An Alabama official, for example, suggested that local law enforcement agencies should not have their own laboratories out of a concern over bias and insufficient resources.[271] The Montgomery Police Department collects DNA evidence, but must send samples to the Alabama Department of Forensic Sciences for analysis.[272] However, two Alabama counties collected voluntarily given blood and mouth swab samples at roadblocks to survey for the presence of alcohol and drugs in the drivers' samples.[273] Officials neglected to disclose whether or not the samples would be retained following the study.[274]

---

of DNA merely upon being charged. *See* DEP'T OF MD. STATE POLICE, *supra* note 256, at 7–8.

269. MD. CODE REGS. 29.05.01.14(J) (2012) ("If an individual whose DNA sample is in the Statewide DNA Database System for a reason other than as a sample collected from an arrestee, any additional sample shall remain in the database and is not subject to automatic expungement."). As to individuals who have been charged and arraigned but not yet convicted, the Act authorizes the state to store both DNA samples and DNA profiles while charges remain pending. §§ 2-506(b), 2-511. If a charge results in a conviction, the DNA sample and DNA profile are retained indefinitely; if the charge does not result in a conviction (or the conviction is later overturned), the state is required to destroy the DNA sample and expunge the DNA profile from its database. *Id.* § 2-511(a)(1), (c).

270. *See* Erin Edgemon, *Law Enforcement Agencies Across Country Amassing DNA Databases; Some Alabama Police Collect DNA, But Don't Keep It*, AL.COM BLOG (updated June 14, 2013, 12:24 PM), http://blog.al.com/montgomery/2013/06/?law_enforcement_agencies_acros.html.

271. *Id.*

272. *Id.*

273. *Id.*

274. *Id.*

III.
SLIPPING THROUGH THE CRACKS: ADVANCES IN TECHNOLOGY AMPLIFY LONG-STANDING DIVISIONS IN SOCIETY BETWEEN GROUPS LARGELY DEFINED BY RACE AND CLASS

The ease of collection, swift processing, and low cost, combined with the opportunity to indefinitely retain DNA samples in underregulated local or state DNA databases, creates a powerful incentive for police to target disfavored individuals for DNA collection. Courts have mostly been unwilling to scrutinize unwarranted search claims arising out of collection from persons who consent to a buccal swab, finding that consent constitutes a waiver of any privacy interest in DNA identification.[275] And, the lack of transparency shields underregulated databases from any meaningful legislative oversight on the utility or disproportionate impact of police collection practices.

As technology advances, lawyers, judges, and lawmakers struggle to deal with the associated changes.[276] The gap between the technology and the law often leads to scenarios that "can potentially conflict with existing social . . . and cultural values."[277] Legislative checks and balances are designed to ensure that laws are a reflection of discourse and debate—they safeguard against reactionary legislation. Emerging technologies do not yet have those safeguards. Once new technology is introduced to the market, the legislature must still follow its lawmaking processes. The rapid pace at which new technologies are created and integrated into society means that even newly enacted legislation may not truly reflect what

275. *See, e.g.*, Garcia-Torres v. State, 949 N.E.2d 1229, 1237–39 (Ind. 2011) (holding that there had been no Fourth Amendment violation because the defendant had voluntary consented to the buccal swab); Pharr v. Commonwealth, 646 S.E.2d 453, 456–58 (Va. 2007) (holding that "[the defendant's] reasonable expectation of privacy in [his buccal DNA] sample ended when he voluntarily provided it to the police for DNA testing and comparison").

276. *See* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 245 ("There is one aspect of technological change . . . that ha[s] the most direct impact on law. This is the capacity of new technology to enable new forms of conduct, including alteration of the means by which similar ends are achieved. . . . Some technological change has a significant impact on what is possible.").

277. *Id.* at 248.

is currently possible.[278] In turn, society is left dealing with legal uncertainty.[279]

Uncertainty is unacceptable when the technology calls into question basic rights—like the right to privacy—and whether or how the government is permitted to utilize new technologies to advance a legitimate governmental interest while still upholding the rights of those affected. Often, cases involving governmental use of new technology are litigated long before the legislature addresses the legal ramifications.[280] Consequently, courts must interpret and apply existing laws to rule on technology questions, but judges are often left trying to apply antiquated laws to novel issues.[281] Courts cannot use today's law to address tomorrow's technology—the courts are limited to interpreting the law as it applies to the facts

278. *Id.* at 249. Although the legislature may attempt to streamline legislation when technological advances demand doing so, the legislative processes themselves require significant time and cooperation among lawmakers holding differing political views. This time gap between technological advances and lawmaking may be interpreted by society as a failure to act in a sufficiently expedient manner, and as a "failure to take action where new technology is perceived to cause harm, threaten social values, or require central planning [and] might well lead to claims that law has fallen behind the times." *Id.*

279. *See id.* at 264 ("It has been said that 'law must be contemporary to be viable.'") (quoting ROBERT E. KEETON, VENTURING TO DO JUSTICE 17 (1969)).

280. *See, e.g.*, United States v. Jones, 132 S. Ct. 345, 962-63 (2012) ("[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After [Katz v. United States, 389 U.S. 347 (1967)], Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute . . . and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law."). In the case of wiretapping, Congress did not enact a statute regulating the practice until forty years after the Court first addressed the issue. *See* Olmstead v. United States, 277 U.S. 438, 466–69 (1928) (holding that wiretapping does not constitute a Fourth Amendment search), *overruled in part by Katz*, 389 U.S. 347; Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–04, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

281. *See* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY 22, 28 (1977) (recognizing that legal rules have "furry edges," and that the rules that come from cases are grounded in certain legal principles, or standards, relied on by judges in articulating support for their legal arguments). Chief Justice Taft himself acknowledged this problem in *Olmstead*:

> Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.

277 U.S. at 465–66.

before it.[282] Accordingly, court decisions address social and legal issues arising from new technology relatively quickly, but often inadequately.[283] The decisions often predate legislation.[284] Once courts create new rules through judicial interpretation, the public is often left guessing how such rulings, based on narrow and specific factual circumstances, apply to other situations left unaddressed by courts and lawmakers. The legislature usually appears content to let the public bear this burden, allowing the judiciary to create laws that govern matters better suited for legislative action.

The task of shaping legal arguments is left, not to politicians, but rather to litigators, because courts necessarily craft legal standards dealing with technological advancements. Litigators craft creative arguments, draw parallels between policy considerations of yesterday's laws and today's problems, and react to issues lawmakers are unable to foresee or address in a timely manner. Laws that do not reflect the advances of society either restrict the way technology may be used or are effectively obsolete.[285]

A. Privacy, Information, and Technology

The indefinite retention in a police database of the DNA profile of a person who has not been arrested for a serious crime or convicted of a felony intrudes upon reasonable expectations of privacy. A person's loss of control over his or her DNA profile in a networked database of state and local databases is harmful because it stigmatizes an individual at the discretion of the police. The privacy interest includes a loss of control over a person's entire DNA sample, which contains highly sensitive, intimate information. For example, there are over 6000 genetic disorders that are severely

282. *See*, Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (limiting its holding to the portion of Maryland's statute authorizing the state to collect DNA samples from arrestees and finding that portion constitutional under the Fourth Amendment).

283. *See, e.g.*, United States v. Jones, 132 S. Ct. 945 (2012) (holding that the attachment of a GPS device to the defendant's car absent a warrant constituted a Fourth Amendment violation); Kyllo v. United States, 533 U.S. 27 (2001) (holding that the use of a thermal imaging device to detect heat radiating from a house is a "search" in part because "the technology in question is not in general public use"); California v. Ciraolo, 476 U.S. 207 (1986) (holding that an expectation of privacy in a home's backyard is unreasonable because a backyard can be observed from an aircraft).

284. *See* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 766 (2005).

285. *See* Moses, *supra* note 276, at 264.

debilitating and stigmatizing.[286] Future testing may include the rapidly expanding field of behavioral genetics in its search to establish causal relationships between genes and a host of adult behaviors related to criminality, such as mental illness, substance abuse, aggression, and impulsiveness.[287] As one commentator put it:

> In its most basic sense, having privacy is having control over our bodies, our possessions, our intimate environment, and the information—whether by watching, listening, touching, or reading—other people can gather about us. The wish for privacy is the wish to control what is revealed about ourselves and our intimate world. . . . Privacy is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention."[288]

The basic notion of "privacy" generally "connotes . . . control over access to the self as well as things close to, intimately connected to, and about the self."[289] Control of one's identity must perforce include a privacy right to protect one's genetic information since DNA is arguably "the human essence—that is, the thing that makes individuals special and perhaps unique."[290] These are substantial and compelling aspects of DNA privacy interests.

New technologies, especially those that make personal information more accessible, make interaction among individuals quicker and more convenient, but they also create a risk to individual privacy—technology brings with it new risks as well as conveniences. Today, digital storage of information for indefinite periods of time increases the likelihood that a person's actions, conversations, or information intended as private may be obtained by

---

286. GENETIC DISEASE FOUND., http://geneticdiseasefoundation.org (last visited Dec. 3, 2014); *see also* NICHOLAS WRIGHT GILLHAM, GENES, CHROMOSOMES, AND DISEASE: FROM SIMPLE TRAITS, TO COMPLEX TRAITS, TO PERSONALIZED MEDICINE 19 (2011) ("More than 6,000 single gene disorders are currently known . . . .").

287. *See* Moses, *supra* note 276, at 249.

288. JANNA MALAMUD SMITH, PRIVATE MATTERS: IN DEFENSE OF THE PERSONAL LIFE 59 (1997) (quoting SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 10–11 (1982)).

289. Sonia Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 746 (2004).

290. Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values*, *in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 49 (Mark A. Rothstein ed. 1997); *see also* Jonathan Kahn, *Biotechnology and the Legal Constitution of the Self: Managing Identity in Science, the Market, and Society*, 51 HAST. L.J. 909, 910 (2000) (arguing that autonomy and self-identity are essential components of the genetic privacy interest in DNA).

others.[291] Such recordkeeping practices allow information about people, in terms of both who they are and what they do, to be accessed by others for decades or perhaps longer.[292]

Although privacy has different meanings depending on the context in which the term is used, an overall concept of the existence of individual privacy is universal.[293] The law fails to keep pace with technology in numerous fields, even on the international stage.[294] In response, many governments have adopted privacy codes that "seek to regulate collection and use of personal data held on file by government and private institutions."[295] Recognizing the law's gross shortcomings has led to certain protections regarding DNA databases on the national and state levels; however, local governments have failed to follow suit and protect their citizens from DNA collection and storage processes that, if attempted at the federal level, would violate federal privacy rights.[296]

In the last century, technology has given the government the ability to peer into private areas of individuals' lives through the use of wiretapping,[297] thermal imaging,[298] GPS tracking,[299] and DNA collection,[300] forcing the Supreme Court to weigh in on whether or not these use of these technologies by law enforcement is constitutionally permissible. The law's inability to protect citizens from law

---

291. *See* James B. Rule, *Privacy Codes and Institutional Record Keeping: Procedural Versus Strategic Approaches*, 37 LAW & SOC. INQUIRY 119, 120 (2012) ("Given the gravity of the consequences, it is no surprise that conflict and controversy have come to surround these [recordkeeping] processes and that legislation and policy have grown up in response.").

292. *Id.* ("Nearly everyone now appreciates how consequential such record keeping is for one's life chances—that is, how much it matters who compiles records, what information can be included, who can share access to such data, and what kinds of decisions can be made on their basis.").

293. *See* Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948), *available at* http://www.un.org/en/documents/udhr/. The concept of a universal idea refers to the general agreement "about the most general and abstract propositions" about that idea. RONALD DWORKIN, LAW'S EMPIRE 70 (1986).

294. *See* Vivek Wadhwa, *Our Lagging Laws*, MIT TECH. REV., July/August 2014, at 11.

295. Rule, *supra* note 291, at 120. Because of the ability to collect and store personal information, "virtually all of the world's liberal societies have adopted some such measures." *Id.*

296. *See* discussion *supra* Parts II.A–B.

297. *See* Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438 (1928), *overruled in part by Katz*, 389 U.S. 347.

298. *See* Kyllo v. United States, 533 U.S. 27 (2001).

299. *See* United States v. Jones, 132 S. Ct. 945 (2012).

300. *See* Maryland v. King, 133 S. Ct. 195 (2013).

enforcement agencies' overreaching use of new technologies has led to outcries for protection, as the use of such technological advances often implicates the constitutional right to be free from unreasonable searches and seizures.[301] In the absence of legislative action, the courts have interpreted law enforcement's use of technologies against the backdrop of society's conception of privacy, and since societal conceptions evolve over time, the outcome of each case has been somewhat inconsistent and often unpredictable.[302]

B. Ethical Issues

1. Expansion of Underregulated DNA Databases Along the Lines of Race

Many factors may lead minorities to be disproportionately represented in local and state DNA databases. First, there are multiple studies that show that police officials on the local level, for example in San Francisco, underreport arrests of minorities.[303] Further, minorities and people of color are disproportionately represented in the criminal justice system.[304] This overrepresentation correlates directly with an overrepresentation of people of color in familial searches given that minorities have a greater and unequal probability of having their DNA collected and stored upon arrest.[305] With the known bias against minority groups and people of color, some scholars believe the familial searches themselves are discriminatory because collection of DNA and the arrest itself is dis-

---

301. *See* cases cited *supra* notes 297–300 and accompanying text.

302. *Id.*

303. *See, e.g.*, *SF Police Underreport Arrest Rates for Latinos, Asians*, THE BAY CITIZEN (Aug. 14, 2012, 12:01 AM), https://www.baycitizen.org/news/policing/sf-police-underreport-arrest-rates/ (finding misclassification of arrestees was the reason for underreporting of minority arrests).

304. *See* Murphy, *supra* note 208, at 321.

305. *See id.* ("First, familial searches of convicted offender and arrestee databases exacerbate the actual and apparent disparities of the criminal justice system, in which people of color are disproportionately represented. Second, the dependence on racial categorization in interpreting DNA typing results transmits a biological determinism about race that is not supported by science and that risks formally inscribing within the justice system inaccurate biases under the legitimizing mantel of scientific truth. And lastly, this widespread acceptance of racial and ethnic categorization as a means of quantifying DNA results (say, allelic frequencies) opens the door to a kind of twenty-first century racial eugenics in which crime and criminology are viewed largely as functions of genetics and biology."); *see also Projects: DNA Databases and Justice*, GENERATIONS AHEAD, http://www.generations-ahead.org/projects/dna-databases-and-justice (last visited Nov. 9, 2014).

cretionary and based on criminal suspicion, which is led by a person's race or ethnicity alone in some cases.[306]

Although the fear of racial discrimination does exist, the U.S. Bureau of Justice Assistance (BJA) insists that DNA specimens in DNA databases do not indicate race and that there is no ability to specify a particular race in a search.[307] Moreover, the BJA emphasizes that law enforcement must comply with constitutional law and other legal ramifications to successfully seize biological evidence; if they do not comply, law enforcement runs the risk of "subsequent suppression of evidence at a trial."[308] The problem with the BJA's assertion is that many local law enforcement agencies have no guidelines directing the collection of DNA and the practice of familial searches.[309]

The concern regarding racial inequality in the criminal justice system has been evident for at least the past 200 years. Nonetheless, the Supreme Court has held that complaints about the personal motivations of the police are irrelevant under the Fourth Amendment.[310] Thus, if a local law enforcement agent detains an individual and collects DNA samples upon an arrest motivated by personal bias, there is the possibility that a court would find that the law enforcement agent would be justified by doing so and protected under the notion that he or she acted on the basis of probable cause.[311] This idea is also connected to the fear that crimes will be underreported: if minorities and people of color ran a higher risk of having their DNA profiles abused by the familial search process, it would be no surprise if they became less likely to report crime.

2. The Crime Gene

The resurgence of the idea of a biological root for criminality has resulted in a massive and disturbing potential for abuse of DNA databases. This troubling ethical question is yet another reason citi-

306. *See, e.g.*, Murphy, *supra* note 208, at 321; Jennifer Mnookin, *The Perils of Expanding DNA Searches to Relatives*, UCLA Newsroom (May 8, 2007), http://newsroom.ucla.edu/stories/070508_dna-perils.

307. *See* Global Just. Info. Sharing Initiative, An Introduction to Familial DNA Searching for State, Local and Tribal Justice Agencies: Issues for Consideration (2012) (analyzing the role of race in DNA databases and familial searches).

308. *Id* at 4.

309. *See* discussion *supra* Part II.A.

310. *See* Whren v. United States, 517 U.S. 806, 806 (1996) ("[T]his Court's cases foreclose the argument that ulterior motives can invalidate police conduct justified on the basis of probable cause.").

311. *See id.*

zens may find themselves targeted in criminal investigations. James Watson, one of the discoverers of the double helix structure of DNA, aptly commented on this possible concern:

> A DNA sample taken for fingerprinting purposes can, in principle, be used for a lot more than merely proving identity: it can tell you a lot about me—whether I carry mutations for disorders like cystic fibrosis, sickle-cell disease, or Tay-Sachs disease. Some time in the not so distant future, it may even tell you whether I carry the genetic variations predisposing me to schizophrenia or alcoholism—or traits even more likely to disturb the peace. Might the authorities, for instance, one day subject me to a more intensive scrutiny than would otherwise be the case simply because I have a mutation in the monoamine oxidase gene that reduces the activity of the enzyme? Some research suggests that this mutation may predispose me to antisocial behavior under certain circumstances. Could genetic profiling indeed become a new tool for preemptive action in law enforcement? Philip K. Dick's 1956 story (which inspired the 2002 movie) "The Minority Report" may not be such far-fetched science fiction as we like to imagine.[312]

In his provocative book, *The Anatomy of Violence*, Adrian Raine details how the scientific community is indeed now returning to a paradigm of human behavior—and in particular criminal behavior—that includes biological roots.[313] Raine argues that the study of the biological roots of criminal behavior, or "neurocriminology," will lead to "effective" techniques, such as preventive detention, that will reduce crime.[314] History is full of examples where science has been used to justify heinous mistreatment of groups of individuals. In the late 1800s, the Italian criminologist Cesare Lombroso proposed that criminals were evolutionary throwbacks who could be identified by primitive features like sloping foreheads and large jaws, and he went on to propose an evolutionary hierarchy of the races, with northern Italians at the apex.[315] Such ideas inspired Mussolini's racial laws in the 1930s and are at the core of some of the ugliest social movements of our time—including forced sterilization of "imbeciles" in the United States through the 1970s.[316] As

312. JAMES D. WATSON & ANDREW BERRY, DNA: THE SECRET OF LIFE 273 (2003).

313. *See* ADRIAN RAINE, THE ANATOMY OF VIOLENCE (2013).

314. *Id.*

315. *See generally* CESARE LOMBROSO, CRIMINAL MAN (1876).

316. *See, e.g.*, Frederick Kunkle, *Sometimes, Sorry May Not Be Enough*, WASH. POST, Jan. 30, 2013, at B1.

the pendulum continues to swing back to a biological basis for criminal behavior, the notion of a database of DNA from criminals is entirely foreseeable and will become an irresistible source of data to study for correlations between genes and criminal behavior.[317] The potential for misuse of DNA information is heightened when the executive branch is permitted, without legislative oversight or judicial approval, to engage in the DNA collection practices at issue in this Article.

C. Chilling Effects

Familial searching of an individual's DNA sample raises fears about intrusions of privacy and potential abuse at all levels. However, these fears are greater at the local level because of the lack of regulations governing local practices, especially because those practices are usually only limited by controlling constitutional authority.[318] Further, the chilling effect of underreporting crime would likely be more prominent at the local level where individuals are more likely to encounter their local law enforcement, as opposed to state or federal agencies. This would be especially likely for victims of crimes where DNA is needed to help catch the perpetrator, and for individuals who would likely turn themselves in for crimes they personally committed. Further, knowledge of familial search practices can hinder community support in crime investigations. Individuals may be less likely to persuade a family member to turn himself in if there is a chance that the individual will be personally tracked through a DNA sample given by the family member. Although there is a notion that innocent individuals have nothing to fear because familial DNA would not result in a hit, there is still the risk of wrongful convictions due to "the multitude of possible errors that can arise during laboratory analysis and data entry; and the great potential for corruption and fabrication."[319] Thus, underreporting of crimes could be an inevitable result of the natural desire to preserve one's privacy.

Moreover, courts have held that CODIS is not designed for intentional familial searches and that local DNA databases are modeled after CODIS. In *United States v. Mitchell*, the court relied on expert opinions that expressed familial searches would not pro-

317. It is noteworthy that the Maryland statute expressly states that one of the legislative purposes of the Maryland DNA Collection Act is to conduct "research." MD. CODE ANN., PUB. SAFETY § 2-505(a)(5) (West 2013).

318. *See* GLOBAL JUST. INFO. SHARING INITIATIVE, *supra* note 307.

319. Kirsten Edwards, *Cold Hit Complacency: The Dangers of DNA Databases Reexamined*, 18 CURRENT ISSUES CRIM. JUST. 92, 92 (2006–07).

duce useful information.[320] If courts have expressed skepticism about familial search practices, it would not be farfetched for individuals to feel the same. At the very least, individuals may feel personally violated as the most intimate aspect of their being—their genetic makeup—is exposed against their will.

Without regulation governing these local databases, people may fear that insurance companies will gain access to the databases. Civil rights and privacy groups are justifiably concerned that the local databases will heighten genetic discrimination and lead to individuals being denied coverage based on findings from stored samples.[321] Although these databases primarily serve law enforcement currently, it is not unconceivable that information may be shared or even sold in the future.

Local DNA databases can also hinder the advancement of clinical research. Individuals may be hesitant to produce their DNA for studies or research if there is a fear their sample could be shared with law enforcement. Individuals commonly volunteer to share their DNA for research advancements and to be used for other purposes. For example, in 2003, Comprehensive Drug Testing Inc. and Quest Diagnostics Inc. collected DNA samples as part of a Major League Baseball survey to study the use of steroids by baseball players.[322] The team owners and players involved voluntarily produced their DNA and agreed in their labor contracts that test results and players' identities would remain confidential.[323] Upon the government's investigation into a local lab cooperative and its role in distributing illegal steroids to players, the DNA samples were seized, leading to investigations of some of the players whose identities were disclosed to authorities.[324] Most importantly, the Ninth Circuit initially held that the government could do so, triggering a subsequent Ninth Circuit panel to raise concerns about the impact on players' privacy.[325]

---

320. 652 F.3d 387, 409 n.19 (3d Cir. 2011) ("[M]ost experts acknowledge that the current iteration of the CODIS software does a poor job of identifying true leads in familial searches.") (citing Murphy, *supra* note 208, at 300).

321. *See* Phillip Bohannon et al., *Cryptographic Approaches to Privacy in Forensic DNA Databases*, *in* PUBLIC KEY CRYPTOGRAPHY 373 (2000) (suggesting that DNA samples can show an individual's health status and deter insurers from covering certain individuals based on their genetic makeup).

322. *See 9th Circuit: Feds Can Keep Seized MLB Drug Test Results:* United States v. Comprehensive Drug Testing, 5 ANDREWS PRIVACY LITIG. REP. 4 (2007).

323. *See id.*

324. *See id.*

325. *See* United States v. Comprehensive Drug Testing Inc., 473 F.3d 915, 919 (9th Cir. 2006) (ruling, as a divided court, that the U.S. government may retain

IV.
EXPANDED DATABASES REQUIRE EXPANDED REGULATION

Proponents of DNA databases have an easy argument. DNA analysis is an effective law enforcement tool,[326] but the analysis takes time, particularly if it has to be performed by a state-run lab that handles analyses for multiple local jurisdictions.[327] Local communities have a vested interest in getting criminals off the streets, a task that is better accomplished sooner rather than later. According to proponents, the tangible crime-fighting benefits of expanding DNA databases at the local level generally outweigh the intangible, fuzzy ethical and privacy problems such an unregulated expansion brings.[328] This expansion is not likely to slow in the wake of the Supreme Court's endorsement of DNA sampling as a type of standard booking procedure in *Maryland v. King*.[329]

---

confidential drug test data seized during raids on two testing laboratories in 2004 for 110 athletes), *opinion withdrawn and superseded on reh'g*, 513 F.3d 1085 (9th Cir. 2008), *reh'g en banc*, 579 F.3d 989 (9th Cir. 2009), *opinion revised and superseded*, 621 F.3d 1162 (9th Cir. 2010). After extensive subsequent litigation, the district court ordered sequestration and the return of copies of the evidence, a ruling that was upheld by an en banc Ninth Circuit panel. *Comprehensive Drug Testing Inc.*, 621 F.3d at 1174 ("Apart from preclusion, however, we cannot see how Judge Mahan abused his discretion by concluding that 'equitable considerations' required sequestration and the return of copies. The risk to the players associated with disclosure, and with that the ability of the Players Association to obtain voluntary compliance with drug testing from its members in the future, is very high. Indeed, some players appear to have already suffered this very harm as a result of the government's seizure. Judge Mahan certainly did not abuse his broad discretion in balancing these equities.") (citations omitted).

326. *But see* Christine Rosen, *Liberty, Privacy, and DNA Databases*, NEW ATLANTIS, Spring 2003, at 37, 40 ("[T]he evidence of DNA's effectiveness as a crime-fighting tool is at once impressive and ambiguous, depending on how the genetic information is used."). A match in a database, on its own, indicates nothing about guilt or innocence but only that two samples are very similar. Guilt and innocence stand as conclusions at the end of an inference, aided by DNA analysis, made by a fallible human being, that may or may not be particularly strong. *See, e.g.*, Osagie K. Obasogie, *High-Tech, High-Risk Forensics*, N.Y. TIMES, July 25, 2013, at A27 (noting cases where DNA database hits and the results of crime scene contamination led to arrests of innocent persons).

327. *See, e.g.*, Goldstein, *supra* note 14 (noting the dramatic crime-solving benefits of local databases and the frustration among local law enforcement personnel regarding how long state crime labs can take to analyze and enter DNA samples, which can be months).

328. *Cf., e.g.*, *id.* (quoting Doug Muldoon, Palm Bay police chief, describing his city's database as "good for law enforcement and good for the community").

329. 133 S. Ct. 1958 (2013). New York University law professor Erin Murphy characterized the ruling this way: "'*King* is a green light. . . . It's a ringing endorse-

As more local law enforcement agencies face real or perceived exigencies regarding community-wide crime prevention, they will push for ever-expanding DNA data on those in their communities. Regulations setting the ethical parameters of the content and use of these databases must keep pace and must cover federal, state, *and* local databases. It is incongruous to think that the policies justifying federal or state regulation don't apply equally to local databases.

Effective regulation of DNA law enforcement databases must strike the right balance between ensuring effective law enforcement and guarding the concerns about the use of unregulated DNA databases.[330] DNA law enforcement databases give the government a unique and exclusive privilege to search a person's most intimately identifying data without that person's approval or knowledge. With that privilege comes the need to use the power appropriately and in line with an individual right of privacy. Appropriate regulations must be crafted to protect against government overreach. Where that institutional right goes largely unregulated, or is regulated in minimal and ineffective ways, there is a greater likelihood for both real and potential abuses of the genetic information stored in DNA databases. Effective regulation should safeguard privacy rights in genetic information and prevent, limit, or mitigate actual and potential abuses that result from institutional control over that information.

To varying degrees, every state regulates the genetic information it acquires, manages, and searches at the statewide level for law enforcement purposes. But, as previously discussed in this Article, the state statutes regulating the management of DNA databases are anything but uniform and most local databases are not subject to any regulatory guidelines.[331] At a minimum, the regulation of a local DNA database should be consistent with the regulation of that jurisdiction's statewide database. Amending an already-existing statutory scheme to achieve consistency across databases would not be

---

ment of DNA testing, and many law enforcement agencies would see this as a dramatic opportunity to expand DNA collection.'" Goldstein, *supra* note 14.

330. *Cf.* United States v. Kincade, 379 F.3d 813, 871 (9th Cir. 2004) (Kozinski, J., dissenting) ("New technologies test the judicial conscience. On the one hand, they hold out the promise of more effective law enforcement and the hope that we will be delivered from the scourge of crime. On the other hand, they often achieve these ends by intruding, in ways never before imaginable, into the realms protected by the Fourth Amendment.").

331. *See supra* Parts I.C, II. According to the head of the Sacramento District Attorney's crime lab, Jill Spriggs, "There really are no rules as to what you can specifically keep. The forensic community is all over the board." Goldstein, *supra* note 14.

difficult, and Alaska, Missouri, and Washington have already explicitly done so.[332]

In order to prevent institutional abuse of local DNA databases and to help protect privacy interests in the genetic information stored in those local DNA databases, effective regulation should have both procedural and strategic components in place.[333] The procedural component should focus on already-acquired genetic samples and encompass the proper use, maintenance, and storage of samples in the database. The strategic component should deal with which genetic samples are entered into and remain in the database; its focus would thus be on policies affecting the acquisition and retention of genetic samples in the database.[334]

Regulations should contain robust expungement provisions to protect an individual's privacy interest in the government's use of her personally identifying information. These provisions could prevent many of the abuses of law enforcement DNA databases.[335] If a DNA sample that qualifies for expungement is removed from the database on the front end, there is nothing to abuse subsequently. The ideal expungement policy would give enough room for effective law enforcement while adequately protecting valuable privacy interests.

Criminal investigations may lead to the collection of a wide range of individually identifying DNA information, but casework samples of known persons should not be entered in a searchable local DNA database. DNA samples of known persons should only be permitted in local DNA databases that are collected pursuant to a state's DNA collection law. Biological samples of victims, mere suspects, and even those who voluntarily offer their cheeks for swab-

332. Alaska, Missouri, and Washington each have "no conflict" statutory provisions that ensure consistency in managing both the local and state DNA databases. ALASKA STAT. § 44.41.035(d) (2014); MO. REV. STA. § 650.057 (2013); WASH. REV. CODE § 43.43.758 (2014). Although the logistical cost is low, implementing consistency in a currently inconsistent system may be difficult, depending on the size of the database and the number of samples subject to expungement at the local level.

333. *See* Rule, *supra* note 291, at 121, for an explanation of strategic approaches.

334. While most statutes contain provisions relating to retention, few statutes provide for oversight of DNA sample collection. *See* Samuels, *supra* note 42, at 22.

335. *See, e.g.*, Amato v. Dist. Att'y for the Cape and Islands Dist., 952 N.E.2d 400, 410 (Mass. App. Ct. 2011) (holding that law enforcement's refusal to expunge an elimination profile in a database derived from a DNA sample voluntarily provided to police during a homicide investigation constituted an "unreasonable, substantial, and serious interference with [the defendant's] privacy" sufficient to state a claim under a state civil law restricting extraneous collection and storage of information by governmental units).

bing for elimination purposes should not be included without meeting statutory requirements. Such a statute should require informed consent confirmed in an authenticated writing, a reasonable basis for the police to request the consent, and the opportunity for the person consenting to qualify for expungement upon request. The state should bear the burden of expunging the record from all national, state, and local databases. Any match that occurs after the date the sample qualifies for expungement should not be used for any purpose. DNA samples collected pursuant to a warrant or court order should be searched in the local and state databases (and the national databank, if a one-time search is permitted) and should be destroyed if the person later qualifies for expungement or if no criminal action has begun within a defined period of time after the collection.

The application of a particular expungement policy to a particular type of DNA sample should be mapped along the spectrum between effective law enforcement and the extent of privacy interests implicated. At one end of the spectrum, convicted felons should receive the least amount of privacy protection and generally should not have the option of being removed from DNA databases. At the other end of the spectrum are voluntarily submitted samples collected for purely elimination purposes; these individuals should receive the most privacy protection since there is no reason to connect them with the crime being investigated. Once the criminal investigatory interest ends or the duration of the investigation reaches a defined point, DNA samples from non-qualifying individuals should qualify for automatic expungement.[336] The same expungement policy that is applied to elimination samples should apply to victim and suspect samples as well. Once a case is closed, there should be no legitimate law enforcement reason for retaining the sample beyond the specific context of the investigation for which the sample was drawn, analyzed, and centralized.

Arrested individuals are arguably entitled to less privacy protection than elimination, victim, or suspect individuals, but to more protection than convicted individuals. Just as the level of justification required to arrest someone for a serious crime is sufficient to warrant an intrusion upon their privacy interests in terms of search and seizure law, it should be sufficient to warrant a comparable in-

336. Retaining elimination samples may save time in investigating future crimes, and law enforcement certainly has an interest in preventing future crimes. However, the better policy would be to limit the retention of such samples to the investigation for which they were acquired. This would prevent open-ended genetic surveillance that would invade the privacy of non-suspected persons.

trusion regarding the retention of someone's genetic information in a public government database only after there has been a judicial finding of probable cause on the qualifying offense to detain the person for trial. If the qualifying charge does not result in a conviction, then the individual should qualify for automatic expungement.

The purpose of DNA analysis and recordkeeping in the law enforcement context is simply to provide a method of identification.[337] The goal is to determine, from the genetic information gathered, who the information belongs to—specifically, to identify an individual using a very basic genetic marker.[338] Conversely, the particular purposes to which DNA analysis and management are put in the private sphere vary, but the general goal is to extract as many details as possible about the person from the genetic sample to create a complete genetic profile.[339]

Private company DNA databases are likely among the most unregulated databases around and contain much more genetic information about the individual than is necessary or permitted for law enforcement purposes like identification.[340] Yet allowing law enforcement to tap into these databases essentially allows an end-run around regulations that pertain only to law enforcement-created samples and database inclusion. The genetic information from private databases is likely to contain much more comprehensive personal information than is necessary only to identify the individual.

Generally, only internal policies of private databases guide how and when they share information with law enforcement.[341] Regulations that restrict the flow of information between the private and law enforcement spheres would help safeguard against abuse and privacy violations. These regulations should prohibit law enforcement from buying, obtaining, or otherwise using private DNA information, whether through voluntary (e.g., direct solicitation) or involuntary (e.g., subpoena) means. This would prevent the criminal investigatory use of information obtained for non-criminal investigatory reasons.

---

337. *See, e.g.*, 42 U.S.C. § 14132 (2012) (titling the section that authorizes the FBI to create and maintain CODIS "Index to facilitate law enforcement exchange of DNA identification information").

338. *See id.*

339. *See, e.g.*, *supra* note 154.

340. *See* Rosen, *supra* note 326, at 42.

341. *Cf.* Sarah B. Berson, *Debating DNA Collection*, NAT'L INST. JUST. J., November 2009, at 9 ("[F]ederal and state privacy laws and penalties that apply to crime labs are stringent—far more stringent than the rules governing private entities that collect blood and saliva for medical or insurance purposes.").

Similarly, law enforcement agencies should not be able to share information with private companies. At all levels, government DNA databases should be prohibited from selling, licensing, or otherwise making available for non-criminal investigatory purposes the genetic information under their control. Because the purposes for acquiring the genetic data should be consistent with their use, private companies should not be able to use compulsorily obtained DNA information used for criminal investigations.

Further, there must be reporting requirements on the collection practices of police to document the effect of different qualifying offense or convictions across various demographics of race, class, age, sex, and geography. The reporting requirements should include disclosure of any discrepancies in the collection of DNA samples and the management and security of the samples and data, such as whether information is stored in the cloud or on an internal server. Police department procedures that govern any DNA database should be deemed public documents that are subject to disclosure upon a public information act request. Additionally, an individual should have the right to inspect the information contained in the database and to challenge its accuracy. These procedural components are essential protections for individual rights.

CONCLUSION

There should be widespread public support for closely regulated DNA databases at the national and state levels. There should also be public acceptance of the premise that an individual who has been convicted or charged with a serious crime has a lesser interest in his DNA profile than the government. So long as law enforcement's focus is solving crimes with identifying genetic features that are not associated with any physical, medical, or behavioral trait, the public may be comfortable with this lesser expectation of privacy. Public support may shift, however, as awareness grows about underregulated state and local DNA databases expanding collection and retention practices to include crime victim DNA, voluntarily provided elimination samples, and surreptitiously collected DNA from persons of interest who may never be charged with a crime. However intermingled with good intentions, the expansion of underregulated local and state DNA databases represents:

> [An] alarming trend whereby the privacy and dignity of our citizens [are] being whittled away by . . . imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite

> unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.[342]

These underregulated state and local DNA databases already intrude upon the privacy rights of crime victims, and the rest of us might not be far behind. As Judge Kozinski of the Ninth Circuit cautioned, "Privacy erodes first at the margins, but once eliminated, its protections are lost for good, and the resultant damage cannot be undone."[343]

In summary, regulation of both state and local DNA databases should exhibit certain minimum features in order to strike a healthy balance between effective law enforcement and the protection of individual privacy interests. Collection practices should include informed consent forms, limitations on future use, and the opportunity to expunge and/or automatic expungement. Regulatory policies should be consistently applied to both the state and local management and use of DNA databases. Automatic expungement policies should be coupled with statutory suppression and applied to different types of DNA samples as follows: elimination, victim, and suspect samples should not be retained or searched in LDIS and should be automatically expunged once the related criminal action has concluded; convicted offender samples and arrestee samples should be automatically expunged if a conviction does not result for the qualifying offense or a conviction is overturned, reversed, pardon, and there is no retrial; and convicted felon samples should be subject to automatic expungement at the conclusion of the sentence or probation. Finally, private entities should not be permitted to use DNA records stored in a law enforcement database for the purpose of predicting medical or behavioral traits or linking DNA records to other databases of information, whether government or private, such as financial records, voting records, motor vehicle records, and Choice Point style databases.

As DNA databases expand their coverage, so too will they continue to advance beyond subpar regulations that are poorly positioned to keep databases in check. In response, meaningful restrictions should balance the need to solve crimes with the otherwise overlooked privacy interests.

---

342. Osborn v. United States, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting).

343. United States v. Kincade, 354 F.3d 813, 871 (9th Cir. 2004) (Kozinski, J., dissenting).