DNA DATABASES, UNIVERSALITY, AND THE FOURTH AMENDMENT

PAUL M. MONTELEONI*

DNA databases enable extremely accurate criminal identification, and a database with appropriate privacy safeguards could be a boon not only for law enforcement but for civil libertarians as well. Unfortunately, current DNA databases lack important precautions and expose DNA donors to serious risks of abuse. The courts that have heard Fourth Amendment challenges to these databases have uniformly upheld them using one of two different rationales. Some courts have held that DNA databases serve a special need, and others have held that the convicted offenders targeted by current statutes have diminished privacy interests in their DNA. However, neither rationale provides a convincing justification for compelling individuals to provide DNA for a database, with or without safeguards. The problem is not with the substantive reasonableness of DNA collection for an ideal database, but with crafting a judicial decision procedure that allows only reasonable databases and not unreasonable ones. The solution proposed by this Note, accordingly, is an alternative decisionmaking procedure that enlists the assistance of the political process. Under the "universality exception" to the warrant requirement proposed by this Note, a search is reasonable if it is authorized by a statute that truly applies equally to every member of the population. The political process leading to the enactment of a universal DNA database, which this exception would require, would ensure that any such database had appropriate safeguards.

INTRODUCTION

Every American state has passed statutes requiring convicted offenders to provide DNA samples for inclusion in a national database of identifying profiles.[1] DNA-based investigation can reduce the risk of false accusations and lessen the need for intrusive physical searches.[2] A DNA database with appropriate safeguards could thus be a boon not only for law enforcement, but for civil libertarians as well.

 A.B., 2001, Harvard University; J.D. candidate, 2007, New York University School of Law. I am indebted to Professors Rachel Barkow, Barry Friedman, James Jacobs, and Stephen Schulhofer, as well as to Christopher Bradley, Dustin Brown, Christopher Deal, Aaron Goldberg, Wangui Kaniaru, Jake Kaufman, Joti Marango, Antoine McNamara, Tara Mikkilineni, Stephen Milligan, Russell Plato, Marc Romanoff, Ben Tolchin, and the staff of the *New York University Law Review*.

[1] For a summary of state DNA database information, see generally SETH AXELRAD, AM. SOC'Y OF LAW, MED. & ETHICS, SURVEY OF STATE DNA DATABASE STATUTES, http://www.aslme.org/dna_04/grid/statute_grid.html (last visited Jan. 8, 2007). For an accompanying explanation, see *id.* http://www.aslme.org/dna_04/grid/guide.pdf (last visited Jan. 8, 2007).

[2] *See infra* Part I.B.1.

Unfortunately, existing DNA database statutes lack such safeguards and may be prone to troubling misuse. As centralized repositories of identifying information, DNA databases may tempt government authorities to expand their uses beyond law enforcement.[3] Worse, current law calls for DNA samples containing the convict's entire genetic code to be retained long after the convict's sentence is complete, which poses a lifelong risk of abuse of this sensitive medical information.[4]

Although convicts have challenged these DNA databases under the Fourth Amendment,[5] every circuit court to consider the issue has upheld the statute in question,[6] often over emphatic dissent.[7] Crucially, however, the circuits have divided as to the rationale justifying the statutes. The Second, Seventh, and Tenth Circuits have found that the databases serve "special needs, beyond the normal need for law enforcement,"[8] thereby invoking a permissive test that balances the government's interest against that of the individual. In contrast, most other circuits have invoked a similar balancing test based solely on their conclusion that the convicted offenders have diminished privacy interests.[9]

Neither of these rationales is convincing. The searches do not serve a "special need" beyond law enforcement, and a finding of diminished privacy interests is entirely conclusory.[10] Indeed, criminal DNA databases do not fit neatly into any existing Fourth Amendment category. They represent a new technology that serves the same law enforcement objectives as traditional investigative techniques, but which bears a different balance of costs and benefits. As the technology does not neatly fit traditional doctrine, the best response the judiciary can muster is to engage in some form of balancing test. An unguided judicial balancing test, however, is too subjective to serve as a reliable decisionmaking procedure to separate appropriately safeguarded databases from undesirable ones, and the reach of such mal-

---

3 *See infra* Part I.B.2.

4 *See infra* note 25 and accompanying text (discussing storage of cell samples); *see also infra* Part I.B.2 (discussing privacy burden).

5 *See infra* Part II.

6 *See infra* notes 69–70 and accompanying text.

7 *See infra* note 157.

8 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring); *see also infra* notes 91–92 and accompanying text.

9 *See infra* Part II.B.

10 *See infra* Part II.A–B.

leable inquiries must be carefully limited if the Fourth Amendment is not to become "one immense Rorschach blot."[11]

The problem, then, is not with the substantive reasonableness of DNA collection for an ideal database, but with crafting a doctrine that distinguishes between reasonable and unreasonable searches. The solution I propose, accordingly, is an alternative approach that enlists the assistance of an unlikely ally in the Fourth Amendment context: the political process. Under my proposal, if a statute produced by a well-functioning democratic legislature requires that *every* member of the population be subject to the search on exactly the same terms and to exactly the same degree, the passage of the statute through the political process provides prima facie evidence that the search in question is reasonable under the Fourth Amendment. This prima facie evidence of reasonableness justifies judges in departing from the warrant requirement and conducting a balancing test to determine whether the search is constitutional. While judges still bear the responsibility of weighing the interests at stake and determining whether the search is reasonable, their inquiry is informed, and the scope of the balancing test is limited, by the political checks that a universal search regime must face. In other words, I propose a narrow "universality exception" to the warrant requirement.

This universality exception could not justify the current criminal DNA database statutes, which only affect a narrow segment of the population. However, it could justify a truly universal DNA database. Such a universal database would face sufficient political checks to ensure the inclusion of necessary safeguards. These political checks would do a better job separating out reasonable from unreasonable database statutes than could any doctrine that relied on the judiciary alone.

The universality exception would apply to other truly universal searches even outside the DNA context, but it would nonetheless be extremely narrow. Very few, if any, conceivable search methods could be fully universalized and still pass through the political process. This is why the political process, such a prominent feature in modern constitutional theory,[12] plays such a small role in Fourth Amendment jurisprudence. The purpose of this Note is not to explore the full interplay between the political process and the Fourth Amendment, but simply to argue that adopting a universality exception would pro-

[11] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 393 (1974).

[12] *See infra* note 142 and accompanying text.

vide a principled way for courts to discriminate between reasonable and unreasonable DNA databases.

Part I describes current criminal DNA databases, evaluates their benefits and costs, and outlines the safeguards that would be required to address current deficiencies. Part II explains how current doctrinal approaches to DNA databases fail to provide a principled justification for any criminal DNA databases, regardless of what safeguards they may have. Part III proposes and defends the universality exception and the prospect of a universal DNA database.[13]

I
CURRENT AND IDEAL DNA DATABASE STATUTES

A. DNA Profiling and Current Statutes

Deoxyribonucleic acid ("DNA") is a complex molecule forming a genetic code integral to an organism's physical development.[14] Each person has DNA expressing a unique[15] genetic code contained in

[13] While numerous commentators have addressed the constitutionality of DNA database statutes and some have argued for universal coverage, I am aware of none that have focused, as I do, on universality as a Fourth Amendment justification for DNA databases. *See, e.g.*, D.H. Kaye, *Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Data from Arrestees*, 34 J.L. MED. & ETHICS 188 (2006) [hereinafter Kaye, *Special Needs*] (arguing that collecting DNA on arrest is constitutional under "biometric identification" exception to warrant requirement); D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413 (arguing that population-wide DNA database would be constitutional under proposed "biometric" exception to warrant requirement); Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and Will) the Supreme Court Do?*, 34 J.L. MED. & ETHICS 165 (2006) (arguing that DNA sampling on arrest is unconstitutional using special needs analysis); Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34 J.L. MED. & ETHICS 153 (2006) (arguing against universal DNA database); Michael E. Smith, *Let's Make the DNA Identification Database as Inclusive as Possible*, 34 J.L. MED. & ETHICS 385 (2006) (advocating broadening DNA databases and destroying tissue samples to protect privacy); Renée A. Germaine, Comment, *"You Have the Right to Remain Silent . . . You Have No Right to Your DNA" Louisiana's DNA Detection of Sexual and Violent Offender's Act: An Impermissible Infringement on Fourth Amendment Search and Seizure*, 22 J. MARSHALL J. COMPUTER & INFO. L. 759 (2004) (arguing DNA collection from arrestees is unconstitutional); Bonnie L. Taylor, Comment, *Storing DNA Samples of Non-Convicted Persons & the Debate over DNA Database Expansion*, 20 T.M. COOLEY L. REV. 509 (2003) (arguing DNA collection from non-convicted persons is unconstitutional).

[14] ROBERT L. NUSSBAUM ET AL., THOMPSON & THOMPSON GENETICS IN MEDICINE 4, 17–18, 23 (6th ed. 2001).

[15] Except for identical twins. Richard Lewontin, *The Genotype/Phenotype Distinction*, *in* THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2004), http://plato.stanford.edu/archives/spr2004/entries/genotype-phenotype/.

every nucleated cell in a person's body.[16] Therefore, a DNA sample found anywhere—in blood, saliva, hair, skin flakes, or other body tissue or fluids—can fruitfully be compared to any known DNA sample.

Standard American forensic DNA analysis examines each sample at thirteen predetermined locations (loci) on the DNA molecule. These loci contain sequences of repeating chemical bases, known as short tandem repeats (STRs).[17] The number of repeats at each locus forms a "DNA profile." This profile is a small set of data that can be compared with great accuracy to the DNA profile generated by STR analysis of any other DNA sample.[18]

STR analysis was intended not to reveal any of a person's genetic traits. A person's full DNA sequence can certainly be analyzed for information regarding his genetic traits,[19] but STRs are measured at loci believed to be "junk DNA," devoid of biological function or significance.[20] In fact, however, DNA profiles do contain some information. In addition to probabilistic correlations between several STRs

---

[16] NAT'L COMM'N ON THE FUTURE OF DNA EVIDENCE, U.S. DEP'T OF JUSTICE, THE FUTURE OF FORENSIC DNA TESTING: PREDICTIONS OF THE RESEARCH AND DEVELOPMENT WORKING GROUP 9–10 (2000), *available at* http://www.ncjrs.org/pdffiles1/nij/183697.pdf [hereinafter COMMISSION REPORT]; *see also* BRUCE ALBERTS ET AL., ESSENTIAL CELL BIOLOGY 268 (2d ed. 2004) (noting that different cell types in multicellular organism contain same DNA).

[17] Peter Gill, *DNA as Evidence—The Technology of Identification*, 352 NEW ENG. J. MED. 2669, 2669–70 (2005).

[18] If, at each locus, Profile 1 has the same number of repeats as Profile 2, the two profiles almost certainly represent the same DNA sequence. While there may be a substantial probability that two DNA sequences have the same number of repeats at any one given locus, the likelihood that the two sets of DNA will match both at that locus and at another is much smaller, and smaller still at a third. The probability that two different random sequences will happen to match at each of thirteen loci is one in one trillion. Gill, *supra* note 17, at 2669. However, DNA sequences are not entirely random, so the likelihood that two matching sequences are from the same DNA is not as high, but still "approaches certainty." COMMISSION REPORT, *supra* note 16, at 1.

[19] *See, e.g.*, NUSSBAUM ET AL., *supra* note 14, at 128–31 (listing genes identified for several diseases). While the function of many genes remains unknown, the amount of information theoretically available is tremendous. "[DNA] contains within its structure the genetic information needed to specify all aspects of embryogenesis, development, growth, metabolism, and reproduction—essentially all aspects of what makes a human being a functional organism." *Id.* at 4. Over 2900 disease genes have already been identified, Weizmann Institute of Science, GeneCards: List of Disease Genes, http://bioinfo.cnio.es/cgi-bin/genecards/listdiseasecards?type=full (last visited Jan. 8, 2007), and scientists can analyze DNA for conditions ranging from heart attack susceptibility and male infertility, *id.*, to earwax consistency, Nicholas Wade, *Scientists Find Gene That Controls Type of Earwax in People*, N.Y. TIMES, Jan. 30, 2006, at A8.

[20] *See, e.g.*, H.R. REP. NO. 106-900, pt. 1, at 27 (2000):

> [T]he genetic markers used for forensic DNA testing were purposely selected because they are not associated with any known physical or medical characteristics . . . . By design, the effect of the system is to provide a kind of genetic

and ethnicity and gender,[21] there appear to be one or two correlations with diseases,[22] and the predictive power of STR analysis will likely increase over time.

All fifty states and federal law compel the collection of DNA from at least some categories of criminal offenders to generate profiles for a DNA database.[23] DNA is usually collected by blood sample or through saliva and inner cheek cells procured by a "buccal swab."[24] The cell samples are generally retained indefinitely in state repositories even after the DNA profile is generated and entered into the database.[25] The state databases are linked to the national Combined DNA Index System (CODIS), which allows access to DNA profiles stored in all state databases and the federal system.[26] Currently, CODIS contains DNA profiles of over 3.5 million offenders.[27]

---

fingerprint, which uniquely identifies an individual, but does not provide a basis for determining or inferring anything else about the person.

[21] COMMISSION REPORT, *supra* note 16, at 35, 40–41.

[22] *See* David Concar, *What's in a Fingerprint?*, NEW SCIENTIST, May 5, 2001, at 9, *available at* http://www.newscientist.com/article.ns?id=dn694 (finding statistically significant links between "junk DNA" and diabetes); Jorge F. Sánchez-García et al., *Multiplex Fluorescent Analysis of Four Short Tandem Repeats for Rapid Haemophilia A Molecular Diagnosis*, 94 THROMBOSIS & HAEMOSTASIS 1099 (2005) (finding variations in short tandem repeats (STRs) correlated with hemophilia); *cf.* Clive Cookson, *Regulatory Genes Found in Junk DNA*, FIN. TIMES (London), June 4, 2004, at 11 (noting that regulatory genes were found in regions of yeast DNA previously thought to be noncoding).

[23] For a summary of state DNA database information, see generally AXELRAD, *supra* note 1. A few criminal DNA database statutes limit DNA collection to those convicted of certain enumerated felonies. *See, e.g.*, Idaho DNA Database Act of 1996, IDAHO CODE ANN. §§ 19-5501 to -5518 (2004 & Supp. 2006). Most (thirty-nine states and the federal criminal system) require collection from all convicted felons. AXELRAD, *supra* note 1. Some also mandate DNA collection from at least some convicted misdemeanants and juveniles adjudicated delinquent. *Id.* Four states (California, Louisiana, Texas, and Virginia) require DNA collection from all persons arrested and charged with certain felonies, *id.*; however, these statutes all have provisions specifying that the DNA profile of an arrestee will be deleted from the databases in the event of an acquittal or dismissal. CAL. PENAL CODE § 299 (West Supp. 2006); LA. REV. STAT. ANN. § 15:614 (2005); TEX. GOV'T CODE ANN. § 411.151 (Vernon Supp. 2006); VA. CODE ANN. § 19.2-310.2:1 (Supp. 2006). The federal government plans to begin collecting DNA from all persons it arrests for crimes or detains for immigration violations. Julia Preston, *U.S. Set to Begin a Vast Expansion of DNA Sampling*, N.Y. TIMES, Feb. 5, 2007, at A1.

[24] *See, e.g.*, OR. REV. STAT. § 137.076 (2005) (specifying DNA collection through blood or oral "buccal" swab).

[25] *See, e.g.*, State Convicted Offender DNA Data Base Act, ARK. CODE ANN. §§ 12-12-1101 to -1120 (2003 & Supp. 2005) (establishing "State DNA Data Bank" as repository of cell samples).

[26] 42 U.S.C. §§ 14131–14135 (2000) (establishing Combined DNA Index System (CODIS)); FED. BUREAU OF INVESTIGATION, CODIS—PARTICIPATING STATES (2006), http://www.fbi.gov/hq/lab/codis/partstates.htm (showing participation in CODIS database by all states).

[27] FED. BUREAU OF INVESTIGATION, CODIS—NATIONAL DNA INDEX SYSTEM (2006), http://www.fbi.gov/hq/lab/codis/national.htm.

B. The Benefits and Costs of Current Statutes

1. Benefits to Society and Civil Liberties

DNA databases provide obvious benefits to law enforcement by generating highly accurate leads.[28] In addition to aiding efficient apprehension of the guilty, DNA databases also benefit the innocent.[29] Solving crimes through DNA matching eliminates pressure to round up scapegoats or perform intrusive searches based on weak evidence.[30] Innocent defendants can petition for exculpatory DNA testing even without a database,[31] but databases provide several significant benefits. First, innocent parties are spared the inconvenience, humiliation, and expense of arrest and prosecution if the police find the true perpetrator through a DNA database. Second, even exculpatory DNA testing does not completely clear an innocent person's name. In many such cases the prosecution and courts may still believe that the innocent party committed the offense with an unidentified accomplice who left the DNA sample.[32] If DNA databases lead police to the actual culprit, this type of false conviction becomes less likely. Considering the intrusiveness and likelihood of error that characterize many police tactics in violent crime investigations,[33] each case in which such tactics are rendered unnecessary by DNA matching is a victory for civil liberties.[34]

---

[28] It is hard to know the magnitude of this benefit, however, due to a lack of empirical evidence. *See* Rothstein & Talbott, *supra* note 13, at 154–55 (noting paucity of empirical evidence on usefulness of databases); *see also* Frederick R. Bieber, *Turning Base Hits into Earned Runs: Improving the Effectiveness of Forensic DNA Data Bank Programs*, 34 J.L. MED. & ETHICS 222, 230–31 (2006) (advocating keeping more systematic data on case outcomes to facilitate evaluation of DNA database efficacy).

[29] *See* Akhil Reed Amar, Op-Ed., *A Search for Justice in Our Genes*, N.Y. TIMES, May 7, 2002, at A31 (noting benefits to innocent of DNA database).

[30] *See, e.g.*, Brown v. City of Oneonta, 221 F.3d 329, 334 (2d Cir. 2000) (describing police dragnet stopping over two hundred black people in small town based on vague suspect description); Saul M. Kassin, *The Psychology of Confession Evidence*, 52 AM. PSYCHOLOGIST 221 (1997) (arguing that police interrogation techniques are deceptive and coercive, and that they induce false confessions).

[31] *Cf.* Justice for All Act of 2004, Pub. L. No. 108-405, § 412, 118 Stat. 2260, 2284–85 (granting money to states to defray costs of postconviction DNA testing).

[32] Amar, *supra* note 29.

[33] *See supra* note 30 and accompanying text.

[34] One commentator has noted the irony of the conservatism implicit in the typical civil libertarian assumption—which he rejects—that the need for new law enforcement powers is always outweighed by the risk of abuse. Solveig Singleton, *Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques*, 30 OHIO N.U. L. REV. 417, 449 (2004).

2. Burden on Privacy

Most courts characterize the impact of DNA collection on privacy as "minimal,"[35] but not all judges or commentators agree that the burden is so slight.[36] As it is impossible to quantify the impact of a burden on privacy, I will begin by comparing DNA collection to the more familiar techniques of drug testing and fingerprinting.

Both DNA collection and drug testing involve removing and chemically analyzing internal bodily material. Both can reveal private medical information.[37] Neither technique directly limits or surveils lawful past, present, or future associations, conversations, personal consumption, travel, or other activities that are constitutionally protected or regarded as private.[38] This is in sharp contrast to most other police searches and seizures, which can reveal information about some or all such activities. However, DNA collection significantly differs from drug testing in that DNA profiles remain on file with law enforcement authorities.[39]

DNA collection also resembles fingerprinting in that it imposes a light but ongoing burden on privacy. Although widespread, fingerprinting is not wholly innocuous.[40] Large collections of data in governmental possession are likely to see their functions, and their size, expand over time.[41] More starkly, a centralized store of identifying

---

[35] *E.g.*, Nicholas v. Goord, 430 F.3d 652, 671 (2d Cir. 2005), *cert. denied*, 2006 WL 2094481 (U.S. Oct. 10, 2006) (No. 06-131); United States v. Kincade, 379 F.3d 813, 839 (9th Cir. 2004) (en banc), *cert. denied*, 544 U.S. 924 (2005); *cf.* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 625 (1989) (noting that process of giving blood does not "infringe significant privacy interests").

[36] *See, e.g.*, *Kincade*, 379 F.3d at 867–68 (Reinhardt, J., dissenting) ("I would hold that the invasion of privacy required by the DNA Act is substantial."); Taylor, *supra* note 13, at 534–37 (discussing privacy burden caused by DNA collection); Germaine, *supra* note 13, at 785 ("DNA extraction from arrestees is arguably just as intrusive and shocking to the conscience as the pumping of a person's stomach without a warrant." (internal citation and quotation marks omitted)).

[37] *See Skinner*, 489 U.S. at 616–17 (analyzing intrusiveness of drug testing); *see also infra* notes 73–74 and accompanying text.

[38] *Cf.* Davis v. Mississippi, 394 U.S. 721, 727 (1969) ("Fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search.").

[39] *See supra* note 25 and accompanying text.

[40] Proposals for a universal fingerprint database, when raised in the past, were widely rejected on civil libertarian grounds. SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION 245–49 (2001); *see also id.* at 249 ("Americans saw the universal fingerprinting movement for what it was: an effort by the state to establish a comprehensive surveillance system over its own citizens.").

[41] *See* Tania Simoncelli & Barry Steinhardt, *California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases*, 33 J.L. MED. & ETHICS 279, 283–84 (2005) (discussing risk of database "function creep"); *see also Kincade*, 379 F.3d at 843 (Reinhardt, J., dissenting) (warning of dangers of centralized governmental recordkeeping); *cf.* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L.

records may make it easier for government to harass or oppress enemies.[42] DNA databases, like fingerprint databases, create a risk of abuse of identifying information.[43]

DNA collection also poses burdens above and beyond those posed by fingerprinting. First, DNA collection is a much better identification technique than fingerprinting, and it is much more difficult to thwart.[44] We constantly shed skin cells, hair clippings, and bodily oils laden with DNA.[45] If forensic technology advances to the point where police officers can recover shed DNA with ease,[46] it might become

---

REV. 1083, 1105–07 (2002) (describing increased dangers to civil liberties posed by increased organization and bureaucratization of law enforcement). Indeed, the consequences of an increase in the size of the database may in fact be even *worse* than the sum of the individual burdens on privacy suffered by each person included in the database, by promoting norms of obedience and chilling the adversarial attitudes necessary for a healthy democracy. I take up such worries in Part III.C, *infra*, when I discuss the prospect of population-wide DNA databases.

[42] *See, e.g.*, *Kincade*, 379 F.3d at 847 (Reinhardt, J., dissenting) ("If placed in the hands of an administration that chooses to 'exalt order at the cost of liberty,' the database could be used to repress dissent or, quite literally, to eliminate political opposition." (citation omitted)); *cf.* Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026, 1039–46 (2003) (discussing risk of "cost-lowering slippery slopes" where innocuous initiatives facilitate later undesirable government actions); Solove, *supra* note 41, at 1105 (discussing risk of certain "government information-gathering shifting power toward a bureaucratic machinery that is poorly regulated and susceptible to abuse"). For an examination of the vulnerability of federal information systems to unauthorized access, see generally Robert Silvers, Note, *Rethinking FISMA and Federal Information Security Policy*, 81 N.Y.U. L. REV. 1844 (2006).

[43] Interestingly, while one common complaint about pervasive databases is the risk of random error, *e.g.*, Singleton, *supra* note 34, at 442–43 (describing difficulty of error correction in technological screening systems); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2001) (suggesting that best metaphor for privacy threat from databases is Franz Kafka's *The Trial*), DNA databases are uniquely protected against this problem. Even if an error leads to an incorrect identification of an innocent suspect, the suspect once identified can ask for a new test of her own DNA against the evidentiary sample, bypassing whatever erroneous information is stored in the database. *See supra* note 31 and accompanying text.

[44] While it is currently costly and time consuming to recover and analyze DNA, this may change. *See, e.g.*, COMMISSION REPORT, *supra* note 16, at 3, 28, 31 (predicting portable kits allowing quick DNA analysis at crime scene by 2010); Kevin Flynn, *Gee-Whiz Police Gadgets Get a Trial Run in New York*, N.Y. TIMES, Mar. 7, 2000, at B1 (describing prototype portable DNA analysis kits and possibility that they would "pay for themselves" through increased efficiency).

[45] *E.g.*, *Kincade*, 379 F.3d at 873 (Kozinski, J., dissenting) ("[W]e can't go anywhere or do much of anything without leaving a bread-crumb trail of identifying DNA matter."); *see also* NAT'L COMM'N ON THE FUTURE OF DNA EVIDENCE, U.S. DEP'T OF JUSTICE, WHAT EVERY LAW ENFORCEMENT OFFICER SHOULD KNOW ABOUT DNA EVIDENCE 3, *available at* http://www.ncjrs.gov/pdffiles1/nij/bc000614.pdf (last visited Nov. 9, 2006) (instructing law enforcement officers to look for sweat, skin, saliva, dandruff, and hair, noting "just because you cannot see a stain does not mean there are not enough cells for DNA typing").

[46] *See, e.g.*, *Kincade*, 379 F.3d at 838 n.37 (noting emerging techniques to extract usable DNA samples from smaller numbers of cells and difficulty of avoiding leaving DNA evidence); JOHN W. BAYNES & MAREK H. DOMINICZAK, MEDICAL BIOCHEMISTRY 481–85

feasible to sweep areas routinely for discarded DNA.[47] If police could sweep the area around a radical mosque or political organization for DNA to determine who had been there, or if they could examine library books to extract DNA from the oils of those who have read them,[48] the lawful behavior of those with DNA profiles in the database might be chilled.[49] Even without such futuristic techniques, DNA profilees might feel cautious about visiting areas that may become crime scenes for fear of becoming suspects in subsequent investigations.[50] The risk of chilling legitimate private activities is thus more pronounced with DNA than with fingerprinting.

Second, DNA collection can also reveal much more personal information than can fingerprinting. As noted in Part I.A, even DNA profiles created by STR analysis can reveal probabilistic information about one's ethnicity and gender, and perhaps more one day.[51] Moreover, all but one of the criminal DNA database statutes permit the retention of the cell samples themselves.[52] A person's entire genetic code can be extracted from these cells, potentially revealing a vast amount[53] of private medical information.[54] These databases thus pose a significant risk of abuse of medical information.[55]

(2d ed. 2005) (describing polymerase chain reaction process and explaining how it allows testing of even miniscule amounts of DNA); *supra* note 44 (describing development of portable DNA analysis kits).

47 I am indebted for this perspective to a discussion with Benjamin Tolchin.

48 A provision of the USA PATRIOT Act currently authorizes federal agents to inspect library records without probable cause, although a limited form of judicial preauthorization is still required. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 106(a)–(d) (2006) (to be codified at 50 U.S.C. §§ 1861(a)–(d)).

49 *See* Solove, *supra* note 41, at 1102–04 (discussing chilling effects caused by lack of anonymity).

50 While this may seem an insubstantial burden, there may well be areas in high-crime neighborhoods, such as particular social clubs or street corners, where violent crimes happen with substantially higher frequency than in other areas. Of course, people in high-crime locations are already at a higher risk of police scrutiny, *see* Illinois v. Wardlow, 528 U.S. 119, 124–25 (2000) (finding defendant's presence in high-crime area and flight from police raised reasonable suspicion), but increasing this risk is not insignificant.

51 It is unlikely that analysis of DNA profiles will ever reveal a great deal of information, however, considering that a profile represents such a small percentage of a person's genetic code. *See supra* notes 17–20 and accompanying text.

52 Wisconsin is the sole exception. WIS. STAT. § 165.77(3) (2003–2004) (requiring samples to be destroyed after analysis has been completed, obtained data has been stored, and applicable court proceedings have concluded).

53 *See supra* note 19 (noting volume of information contained within DNA).

54 *See, e.g.*, Maxwell J. Mehlman, *The Privacy of Genetic Information*, THE DOCTOR WILL SEE YOU NOW, Oct. 1999, http://www.thedoctorwillseeyounow.com/articles/bioethics/geneticinfo_1/ (noting provisional consensus among bioethicists that genetic information should not be disclosed to third parties without patient's consent).

55 Risk of abuse is relevant not only in policy analysis but also under the Fourth Amendment. In *Skinner v. Railway Labor Executives' Ass'n*, the Court took note of the fact that urine collected in a drug testing program could be tested for more than the mere

Most criminal DNA database statutes forbid using DNA profiles for purposes other than criminal identification and impose sanctions on any such abuse,[56] but it is difficult to know how stringently these prohibitions will be enforced. It seems unlikely that policymakers will allocate significant investigative or prosecutorial resources toward protecting the genetic privacy of convicted offenders against abuse by law enforcement. For these reasons, DNA databases impose substantial burdens on privacy that are more severe than those created by drug testing or fingerprinting.[57]

C. Neglected Privacy Safeguards

Current DNA databases impose substantial burdens on privacy by exposing DNA profilees to the risk of abuse not only of identifying information but also of medical information. A more careful DNA database statute could address these concerns through two main safeguards to minimize the risks of abuse. The first, and most obvious, is destruction of the cell samples themselves.[58] While it might be conve-

presence of drugs and thereby implicate Fourth Amendment privacy interests. 489 U.S. 602, 617 (1989); *see also* Payton v. New York, 445 U.S. 573, 589 (1980) (factoring likelihood of police disregarding search limitations into analysis of search's reasonableness). For the view that "the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information even after a lawful seizure," see Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995).

[56] *See* AXELRAD, *supra* note 1 (summarizing penalties authorized by state statutes). The federal government has also encouraged some privacy protection by allowing access to CODIS only to states which agree to meet quality assurance benchmarks for their DNA analysis, 42 U.S.C. § 14132(b)(1) (2000), to have their laboratories undergo accreditation and periodic audits, § 14132(b)(2) (2000 & Supp. IV 2004), to allow disclosure of the DNA profile data only for specified authorized purposes, § 14132(b)(3) (2000), and to provide a mechanism for expunction of DNA records based on overturned convictions or arrests resulting in final dispositions other than convictions, § 14132(d)(2) (2000 & Supp. IV 2004) (as amended by Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1002(3) (2006)).

[57] There is an additional respect in which DNA databases arguably infringe on privacy in a way that fingerprints do not. DNA is a key component of human growth and development, and many people see it as integral to who they are. The mere possession of a repository of such specific and personal information could be seen as an infringement on that person's privacy even if there is no risk that the information will ever be studied. (I am indebted for this argument to a conversation with Benjamin Tolchin.) However, while this view is consistent with popular sentiments attributing an almost supernatural quality to DNA, *e.g.*, Germaine, *supra* note 13, at 759 ("'Isn't my DNA the only thing that makes me unique from everyone else in the world?'"), people do not in fact appear to care whether or not their hair clippings or shed skin cells find their way into the possession of other parties, so long as they are confident that nobody will actually use these cells to study their DNA. This objection is probably better cast as a concern with even a de minimis risk of abuse of medical information.

[58] Several scholars agree that sample destruction would be beneficial. *E.g.*, David Lazer & Viktor Mayer-Schönberger, *Statutory Frameworks for Regulating Information*

nient for law enforcement to be able to practice new analysis techniques without resampling all of the DNA donors,[59] this purely administrative convenience should not weigh heavily against the privacy interests burdened by sample retention.[60] And while there is some quality control benefit to retaining the samples, the same effect could be achieved at somewhat greater expense through less troubling means.[61]

Safeguards could also be developed to mitigate the risk of abuse of identifying information. One might worry, for example, that the police would attempt to track an individual solely to harass her, or that police would attempt to identify members of controversial organizations by searching meeting places for DNA.[62] This concern can be addressed without impeding lawful investigations: The DNA profiles would be identified only by anonymous code numbers, and a master list of the identities associated with the code numbers would be maintained by a separate agency.[63] To access identities contained on the master list, law enforcement officers would be required to apply for a court order. A judge would review an affidavit in which officers would allege facts showing probable cause to believe that the person whose identity they sought committed a crime. That is, officers would

Flows: Drawing Lessons for the DNA Data Banks from Other Government Data Systems, 34 J.L. MED. & ETHICS 366, 372 (2006) (advocating sample destruction as "hardwired constraint" on government's use of data); Rothstein & Talbott, *supra* note 13, at 159 (advocating sample destruction to assure public that DNA information will not be misused); Smith, *supra* note 13, at 388 (advocating sample destruction as "solution to the privacy problem"). *But see* M. Dawn Herkenham, *Retention of Offender DNA Samples Necessary to Ensure and Monitor Quality of Forensic DNA Efforts: Appropriate Safeguards Exist to Protect the DNA Samples from Misuse*, 34 J.L. MED. & ETHICS 380, 383 (2006) (asserting adequacy of existing safeguards against abuse of samples).

[59] *See* COMMISSION REPORT, *supra* note 16, at 36 (discussing this rationale for preserving DNA samples).

[60] Law enforcement need not suffer. Although resampling all of the DNA donors would delay the transition to a new database based on the new analysis techniques, any existing database could be maintained and searched until the transition was complete.

[61] Current practices call for reanalysis of the stored sample upon finding a match to guard against the possibility that the stored profile is inaccurate. Herkenham, *supra* note 58, at 381–82. However, the same degree of quality assurance could be attained by simply conducting two independent STR analyses at the outset, storing the resulting profiles separately, and destroying the sample. While this would be more expensive in that it would require two STR analyses to be performed on all stored samples, this expense would be partially offset by the saved costs of storing the sample. And as STR analysis becomes less expensive, *supra* note 44, this procedure might eventually be cheaper on net.

[62] *See supra* notes 48–49 and accompanying text.

[63] The federalist structure of current DNA databases complicates matters somewhat. On the most simple conception, one federal agency would maintain a master list that would be available to all state agencies. If the states wished to maintain access to the identities themselves, however, each state would have an agency containing its master list of identities.

have to convince the judge that they were conducting a criminal investigation in which they recovered DNA evidence and that STR analysis revealed a match in the database with the code number. If law enforcement made this showing, the judge would order disclosure of the identity associated with that code number.[64]

The court order requirement would ensure that law enforcement officers sought an individual's identity for a legitimate reason, not simply for harassment or other impermissible motives.[65] This second safeguard would not only minimize the risk of direct abuse of identifying information, it would also protect against gradual "function creep"[66] by requiring any changes in the standard for granting such court orders to be legislative or judicial. Law enforcement could not unilaterally decide to employ DNA databases for new purposes.[67]

---

[64] *Cf.* K.A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 197–202 (2004–2005) (advocating "pseudonymity" as technique to avoid unnecessarily infringing on privacy).

[65] If this affidavit requirement were unduly burdensome, perhaps a court order could issue upon the officers' certification that they were conducting an authorized investigation into a crime and that the number corresponding to the identity sought matched a profile taken from a sample collected in that investigation. There is, however, no apparent reason an affidavit would be unduly burdensome to prepare, especially if the police could obtain information based on a certification of exigent circumstances, pending later presentation of a full affidavit.

[66] *See supra* note 41 and accompanying text.

[67] *See* Lazer & Mayer-Schönberger, *supra* note 58, at 372–73 (advocating "administrative speed bumps" as means of avoiding "large scale re-purposing" of DNA data). Indeed, this arrangement would allow legislatures, if they wished, to restrict DNA database searches to investigations of certain types of offenses. *Cf.* 18 U.S.C. § 2516(1) (2000, Supp. I 2001 & Supp. III 2003) (amended by USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 113, 120 Stat. 192, 209 (2006) (to be codified at 18 U.S.C. § 2516(1))) (limiting authorized government electronic surveillance in criminal investigations to enumerated predicate offenses).

One might object that whether or not it is permitted by law, the President acting in the name of national security could merely order the agency with the master list to disclose its contents and thereby circumvent this protection. This is a risk, but we do not normally ban a technology due to the fear that no law can prevent the executive from misusing it. For example, wiretapping poses a more significant danger to privacy than maintenance of DNA profiles, *cf. supra* text accompanying note 38, and the fact that the government has access to electronic surveillance equipment creates the risk that it will violate the federal wiretapping statute by using this equipment without following statutory safeguards, *see* 18 U.S.C. § 2511 (2000, Supp. I 2001 & Supp. III 2003) (prohibiting purely domestic electronic surveillance except under specific statutory authorization); 50 U.S.C. § 1809 (2000) (similar for foreign intelligence electronic surveillance); *see also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (describing National Security Agency (NSA) warrantless surveillance program); Curtis Bradley et al., Letter, *On NSA Spying: A Letter to Congress*, N.Y. REV. BOOKS, Feb. 9, 2006, at 42 (arguing that NSA surveillance program "appears on its face to violate existing law"). I am aware of nobody who suggests that Congress remove this risk by outlawing the possession or manufacture of all electronic surveillance equipment. The fact that we are relatively

Taken together, these safeguards would minimize the privacy burdens imposed by DNA databases without interfering with legitimate law enforcement. Unfortunately, legislatures are unlikely to adopt these safeguards on their own. Furthermore, as I will argue in the next Part, neither current databases nor databases with my suggested safeguards fit well into current Fourth Amendment doctrine.

II

THE POOR FIT BETWEEN FOURTH AMENDMENT DOCTRINE AND CRIMINAL DNA DATABASE STATUTES

Since their inception, criminal DNA database statutes have survived challenges on several constitutional grounds.[68] Plaintiffs subject to these statutes have argued that mandatory DNA sample collection and profile retention in a database amount to unreasonable searches or seizures within the meaning of the Fourth Amendment.[69] All circuits that have heard such challenges have rejected them,[70] albeit on two different rationales. Neither rationale, however, provides a prin-

untroubled by the existence of technology that can be misused may indicate a belief that over the long run the executive will generally not blatantly defy the specific commands of Congress. And to the extent that the executive really is wholly unbound by law, this is a problem not just for DNA databases but for any limited government.

[68] Although I will not address such challenges here, courts have uniformly rejected challenges based on the Self-Incrimination Clause of the Fifth Amendment, *e.g.*, Boling v. Romer, 101 F.3d 1336, 1340 (10th Cir. 1996), the Equal Protection Clause of the Fourteenth Amendment, *e.g.*, Roe v. Marcotte, 193 F.3d 72, 82 (2d Cir. 1999), the Free Exercise Clause of the First Amendment, *e.g.*, Shaffer v. Saffle, 148 F.3d 1180, 1181–82 (10th Cir. 1998), the Due Process Clause of the Fifth Amendment, *e.g.*, Vore v. U.S. Dep't of Justice, 281 F. Supp. 2d 1129, 1138 (D. Ariz. 2003), the Cruel and Unusual Punishment Clause of the Eighth Amendment, *e.g.*, Kruger v. Erickson, 875 F. Supp. 583, 587–88 (D. Minn. 1995), the Ninth Amendment, *e.g.*, *Boling*, 101 F.3d at 1340, the constitutional separation of powers, *e.g.*, United States v. Sczubelek, 402 F.3d 175, 189 (3d Cir. 2005), *cert. denied*, 126 S. Ct. 2930 (2006), and the Ex Post Facto Clause of Article I, *e.g.*, *Shaffer*, 148 F.3d at 1182.

[69] *See, e.g.*, United States v. Kraklio, 451 F.3d 922, 923 (8th Cir. 2006); Nicholas v. Goord, 430 F.3d 652, 656 (2d Cir. 2005), *cert. denied*, 127 S. Ct. 384 (2006); *Sczubelek*, 402 F.3d at 182; Padgett v. Donald, 401 F.3d 1273, 1276 (11th Cir. 2005), *cert. denied sub nom.* Boulineau v. Donald, 126 S. Ct. 352 (2005); United States v. Kincade, 379 F.3d 813, 821 (9th Cir. 2004) (en banc), *cert. denied*, 544 U.S. 924 (2005); Green v. Berge, 354 F.3d 675, 676 (7th Cir. 2004); Groceman v. U.S. Dep't of Justice, 354 F.3d 411, 412–13 (5th Cir. 2004); *Boling*, 101 F.3d at 1338; Jones v. Murray, 962 F.2d 302, 305 (4th Cir. 1992), *cert. denied*, 506 U.S. 977 (1992).

The Fourth Amendment states in part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

[70] The Supreme Court has not yet addressed any challenges to criminal DNA database statutes. See the denials of certiorari listed in note 69, *supra*.

cipled justification for upholding any criminal DNA database statute,[71] let alone the databases in their current form.

All circuits agree that the forcible collection of cellular material amounts to a search within the meaning of the Fourth Amendment.[72] This follows from the Supreme Court's holding, in *Skinner v. Railway Labor Executives' Ass'n*, that the required submission and subsequent analysis of internal bodily fluids "infringes an expectation of privacy that society is prepared to recognize as reasonable" and constitutes a search under the Fourth Amendment even if there is no actual "surgical intrusion into the body."[73]

Even though courts agree that compulsory DNA collection constitutes a search, the Fourth Amendment "does not proscribe all searches and seizures, but only those that are unreasonable."[74] The Supreme Court has long held that searches pursuant to a warrant issued upon probable cause are presumptively reasonable,[75] while warrantless searches are presumptively unreasonable.[76] However,

---

[71] As will become apparent in Part II, *infra*, either rationale could justify a DNA database statute that authorized retention of DNA profiles only until such time as the donor was released entirely from all criminal justice supervision. But such a database would not truly be a criminal DNA database in the sense I am describing, as it would have limited usefulness for general crime control and thus would be better characterized as serving the special need of administering a correctional system. *See infra* note 114 and accompanying text (describing special need of facilitating rehabilitation).

[72] *Kraklio*, 451 F.3d at 923 (Eighth Circuit); *Nicholas*, 430 F.3d at 658 (Second Circuit); *Sczubelek*, 402 F.3d at 182 (Third Circuit); *Padgett*, 401 F.3d at 1277 (Eleventh Circuit); *Kincade*, 379 F.3d at 821 n.15 (Ninth Circuit); *Green*, 354 F.3d at 676 (Seventh Circuit); *Groceman*, 354 F.3d at 413 (Fifth Circuit); *Boling*, 101 F.3d at 1340 (Tenth Circuit); *Jones*, 962 F.2d at 306 (Fourth Circuit).

[73] 489 U.S. 602, 616–17 (1989). The question might be harder if a court were confronted with a DNA statute authorizing only the collection of dead skin flakes with a sticky pad applied to one's arm, as the dead skin collected is external and often shed inadvertently. One might argue that such a method of collection was not a search, as it merely collected that which a person knowingly exposed to the outside world. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."). However, the *Skinner* Court also noted that chemical analysis of body tissue to obtain physiological data invokes the Fourth Amendment even independent of the intrusiveness of collecting the tissue. *Skinner*, 489 U.S. at 616. This would seem to subject even a regime collecting skin flakes with a sticky pad to the Fourth Amendment. *See Nicholas*, 430 F.3d at 656 n.5 (adopting this interpretation of *Skinner*). The detention of the person necessary to collect tissue is also a Fourth Amendment seizure. *Skinner*, 489 U.S. at 616; *see also* Davis v. Mississippi, 394 U.S. 721, 727 (1969) (finding that detention for sole purpose of obtaining fingerprints is subject to Fourth Amendment).

[74] *Skinner*, 489 U.S. at 619.

[75] *But see* Winston v. Lee, 470 U.S. 753, 755 (1985) (holding surgical extraction of bullet from defendant to be unreasonable search and seizure even when conducted pursuant to warrant).

[76] *See, e.g.*, *Skinner*, 489 U.S. at 619 (noting that in most criminal cases, search or seizure "is not reasonable unless it is accomplished pursuant to a judicial warrant issued

there are several exceptions to this general requirement of a warrant and probable cause. A warrantless search may be found reasonable if conducted, inter alia, incident to a lawful arrest,[77] in an automobile,[78] in hot pursuit of a suspect,[79] or during an emergency such as a fire.[80] Because DNA collection is performed without a warrant, it can only be justified if it fits within such an exception.

Courts have invoked two separate exceptions to the warrant requirement when upholding criminal DNA database statutes.[81] One justifies a search if it furthers a special need beyond law enforcement and if the government's interest outweighs the burden on privacy. The other justifies a search if the search target's privacy interest is diminished in the eyes of the law and if the government's interest outweighs the burden on privacy.

A. The Special Needs Rationale

The special needs exception to the warrant requirement justifies certain warrantless and suspicionless searches.[82] If a search is conducted pursuant to "special needs, beyond the ordinary need for law enforcement,"[83] its reasonableness is analyzed by balancing the state's interest in conducting the search against the individual's interest in

upon probable cause"); United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 317–18 (1972) (holding that outside of "carefully delineated" exceptions to warrant requirement, warrantless searches and seizures are unlawful even if law enforcement agents acted reasonably).

77 *See, e.g.*, Agnello v. United States, 269 U.S. 20, 30 (1925) (noting that governmental right to conduct warrantless search incident to arrest is "not to be doubted").

78 *See, e.g.*, Carroll v. United States, 267 U.S. 132, 149 (1925) (upholding warrantless search of automobile).

79 *See, e.g.*, Warden v. Hayden, 387 U.S. 294, 298–99 (1967) (upholding warrantless entry into residence in hot pursuit of armed suspect).

80 *See, e.g.*, Michigan v. Tyler, 436 U.S. 499, 509 (1978) (upholding warrantless entry into burning building).

81 I refer to the requirement of a warrant and probable cause as the "warrant requirement" for simplicity even though some exceptions to the warrant requirement still require probable cause. As I discuss in Part II.A and II.B, *infra*, both rationales used by the circuit courts are exceptions to both the requirement of a warrant and the requirement of probable cause.

82 *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (upholding suspicionless drug testing of high school athletes as serving special need of furthering school discipline); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (upholding suspicionless highway checkpoints as serving special need of removing drunk drivers from road); New York v. Burger, 482 U.S. 691, 712 (1987) (upholding suspicionless search of automobile junkyard as serving special need of enforcing regulatory scheme applied to closely regulated industry); United States v. Martinez-Fuerte, 428 U.S. 543, 556–57 (1976) (upholding suspicionless border checkpoints based on need to secure borders from aliens and smugglers).

83 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

being undisturbed.[84] The Supreme Court has made clear that to come within the special needs exception, a search cannot simply serve "the general interest in crime control."[85] In *City of Indianapolis v. Edmond*, the Court found that a system of checkpoints primarily intended to interdict illegal narcotics did not qualify for the special needs exception because it served only the general need for law enforcement.[86] Similarly, in *Ferguson v. City of Charleston*, a program testing expectant mothers' urine in hospitals for cocaine was invalidated as authorizing unreasonable searches and seizures because its primary purpose was related to law enforcement.[87]

The Second, Seventh, and Tenth Circuits consider the construction of a DNA database to serve a special need, thus allowing warrantless DNA collection to escape the presumption of per se unreasonableness.[88] In conducting the balancing test, these circuits have uniformly found that the state's interest outweighs the individual's, and they have upheld the criminal DNA database statutes as a result.[89]

The need identified in these cases is the state's purpose in gathering evidence relevant to solving potential future crimes.[90] This purpose was most clearly identified by the Second Circuit in *Nicholas v. Goord*.[91] Analyzing legislative history and governmental public statements, the court concluded that the New York DNA database

[84] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989) ("[W]here a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."); *see also infra* note 110 (noting that "privacy expectations" do not refer to actual expectations but rather to privacy interests).

[85] City of Indianapolis v. Edmond, 531 U.S. 32, 42 (2000).

[86] *Id.* at 44 ("We decline to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes.").

[87] 532 U.S. 67, 83 (2001).

[88] Nicholas v. Goord, 430 F.3d 652, 655 (2d Cir. 2005), *cert. denied*, 127 S. Ct. 384 (U.S. Oct. 10, 2006) (No. 06-131); Green v. Berge, 354 F.3d 675, 677–78 (7th Cir. 2004) (citing Shelton v. Gudmanson, 934 F. Supp. 1048, 1050–51 (W.D. Wis. 1996)); United States v. Kimler, 335 F.3d 1132, 1146 (10th Cir. 2003) (citing Miller v. U.S. Parole Comm'n, 259 F. Supp. 2d 1166, 1176 (D. Kan. 2003)).

[89] The factors considered in the balancing test are the state's interest in accurately investigating and prosecuting crimes, and the individual's privacy interests, including both the burden the search may impose on the individual's privacy and any diminution her privacy interests may suffer. *See, e.g.*, *Nicholas*, 430 F.3d at 669–70 (weighing government's interest, burden on prisoners' privacy, and prisoners' diminished privacy interest); *Miller*, 259 F. Supp. 2d at 1177–78 (same).

[90] *Nicholas*, 430 F.3d at 668; *Green*, 354 F.3d at 678 (citing *Shelton*, 934 F. Supp. at 1050–51); *Kimler*, 335 F.3d at 1146 (citing *Miller*, 259 F. Supp. 2d at 1176).

[91] 430 F.3d at 668.

statute's primary purpose was to gather information that would aid in the investigation and prosecution of future crimes.[92]

On its face, gathering information for use in investigating and prosecuting future crimes seems indistinguishable from the general need for effective law enforcement.[93] However, the Second Circuit found that the Supreme Court had raised the possibility in *Illinois v. Lidster* that some types of law enforcement actions, in particular "information-seeking" searches and seizures, might nonetheless serve a special need.[94]

In *Lidster*, the Court considered police roadblocks set up to question motorists about whether or not they had seen a hit-and-run accident.[95] Although the police were gathering this information precisely so that they could investigate and prosecute a crime, the suspicionless seizures[96] were upheld as "information-seeking."[97] In finding a special need, the Court relied on the fact that the police were not seeking to incriminate any of the stopped motorists, but rather another

[92] *Id.* (citing Nicholas v. Goord, No. 01 Civ. 7891, 2003 WL 256774, at *12 (S.D.N.Y. Feb. 6, 2003) (Gorenstein, Mag. J.)); *see also* New York State Division of Criminal Justice Services, New York State DNA Databank Frequently Asked Questions, http://criminaljustice.state.ny.us/forensic/dnafaqs.htm (last visited Jan. 23, 2006) ("The primary function of the DNA Databank is to maintain DNA profiles of convicted offenders that can be used by law enforcement to identify a perpetrator of a crime when DNA evidence is retrieved from a crime scene."). This seems to be a fair characterization of this and all of the various criminal DNA database statutes, none of which tries to disguise its primary purpose of solving crimes. *E.g.*, DEL. CODE ANN. tit. 29, § 4713(f) (2005) (providing that purpose of DNA database is to identify perpetrators of crime). Judge Gould, in his concurrence in *Kincade*, suggested that the DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106-546, 114 Stat. 2726 (2000), served the special need of supervising releasees. United States v. Kincade, 379 F.3d 813, 840 n.2 (9th Cir. 2004) (en banc) (Gould, J., concurring), *cert. denied*, 544 U.S. 924 (2005). But given the scant attention these statutes pay to the supervised release or parole relationship, and especially the retention of the DNA profile after the individual leaves the criminal justice system entirely, this is not a persuasive primary purpose for this or any other criminal DNA database statute. *Kincade*, 379 F.3d at 855–59 (Reinhardt, J., dissenting) (arguing that primary purpose of same Act is not supervising releasees). For more detailed analysis of why various purported purposes of criminal DNA database statutes are not in fact their primary purposes with respect to the special needs rationale, see generally Maclin, *supra* note 13.

[93] Judge Leval recognized this in his *Nicholas* concurrence. 430 F.3d at 673 (Leval, J., concurring) ("Were *Edmond* and *Ferguson* the last word on the matter, it would be difficult to reconcile approval of the New York DNA Statute, whose purpose is to collect identifying evidence for use in criminal prosecution, with the broad rule of presumptive unconstitutionality announced in those cases."); *see also supra* notes 85–87 and accompanying text (discussing *Edmond* and *Ferguson*).

[94] *Nicholas*, 430 F.3d at 663 (quoting Illinois v. Lidster, 540 U.S. 419, 424 (2004)).

[95] *Lidster*, 540 U.S. at 422.

[96] In *Nicholas*, the Second Circuit noted that *Lidster* did not distinguish between searches and seizures for Fourth Amendment purposes. *Nicholas*, 430 F.3d at 663 n.21.

[97] *Lidster*, 540 U.S. at 424.

party.[98] This removed the stop's purpose from the heart of the state interest in crime control, and the Court found these seizures reasonable after balancing the interests involved.[99]

In *Nicholas*, the Second Circuit relied on *Lidster*'s reasoning to classify the searches authorized by New York's criminal DNA database statute as serving a special need despite their law enforcement purpose.[100] In particular, the court found that the lack of a specific crime under investigation distinguished DNA collection from general law enforcement activity.[101] Further, the court found that the information obtained by DNA collection bears only on identity and does not incriminate anyone.[102] These factors led the Second Circuit to conclude that the collection of information potentially useful in the investigation and prosecution of future crimes is a special need, triggering a balancing test that ultimately favors DNA collection.

Nicholas ultimately fails to convince. First, the fact that target information merely pertains to identification of a guilty person does not prevent a search from furthering a law enforcement purpose. Under the Fourth Amendment, there is no distinction between evidence that only bears on identity and other evidence. Suppose police learn that the culprit in a past assault wore a distinctive yellow shirt and wish to search a suspect's residence for it. Absent exigent circumstances, the police's search of the residence to find the shirt would be automatically unreasonable without a warrant. Yet the shirt is relevant only to establishing the suspect's identity. No one could argue that this would be a "special needs" search—to do so would give the government free reign over all private spaces. Like any other law enforcement search, it is subject to the requirements of a warrant and probable cause. Seeking information relevant "only" to criminal identification simply does not manufacture a special need.

---

[98] This finding was explicit:

> The stop's primary law enforcement purpose was *not* to determine whether a vehicle's occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others. The police expected the information elicited to help them apprehend, not the vehicle's occupants, but other individuals.

Id. at 423; *see also id.* at 424–25 (relying on this finding to reject application of *Edmond*-type rule of presumptive unconstitutionality to "brief, information-seeking highway stops").

[99] *Id.* at 427–28.

[100] *Nicholas*, 430 F.3d at 668–69.

[101] *Id.* This ground was also noted by the Seventh Circuit in *Green v. Berge*, 354 F.3d 675, 678 (7th Cir. 2004), and by the Tenth Circuit—albeit obliquely—in *United States v. Kimler*, 335 F.3d 1132, 1146 (10th Cir. 2003).

[102] *Nicholas*, 430 F.3d at 669 (noting that DNA samples "in fact provide no evidence in and of themselves of criminal wrongdoing" (citation and internal quotation marks omitted)).

Second, the factors distinguishing *Lidster* from *Edmond* also distinguish *Lidster* from the DNA collection cases. Surely the greatest factor distinguishing *Lidster*, where the Court found a special need, from *Edmond* and *Ferguson*, where it found none, is that in *Lidster* the police's seizures were not performed for the purposes of investigating the seized motorists.[103] In *Lidster*, the Court repeatedly emphasized that the police were gathering information from some motorists to investigate *other* motorists.[104] In *Edmond* and *Ferguson*, by contrast, the searches sought information intended to be used against the search targets themselves. While criminal DNA database statutes are unlike the search regimes in *Edmond* and *Ferguson* in that they are not aimed at investigating past or present crimes, they are certainly aimed at eventually incriminating the search *target*. They are thus closer to the searches in *Edmond* than to the seizures in *Lidster*.

Third, it is unclear why investigating future crimes is a special need and not a general law enforcement need. It is strange to read *Lidster*, which considered police investigation of a specific crime, as standing for the proposition that the *absence* of a specific crime under investigation creates a valid special need. Future crimes are inherently speculative, and investigation of potential future crimes is prone to abuse. This is implicit in the general requirement of a warrant and probable cause for searches and seizures.[105] Indeed, a factor that counted in the government's *favor* in *Lidster* was that "the stop's objective was to help find the perpetrator of a specific and known crime, not of unknown crimes of a general sort."[106]

DNA collection may be less invasive than many other types of searches,[107] but at any given level of governmental intrusion, the

---

[103] Of course this rationale, if extended further, would exempt all searches seeking information about third parties from the warrant requirement. But even if the Court is not likely to employ this analysis in all future cases, it certainly did so in *Lidster*. *See supra* note 98 and accompanying text (showing Court's reliance on this factor).

[104] One might doubt that this was truly the purpose of the search, given that the roadblock was presumably intended to put the police in a position to question motorists who were present at the time of the accident. Illinois v. Lidster, 540 U.S. 419, 422 (2004). As the actual culprit was obviously a motorist present at the time of the accident, the police might really have been looking for him. However, the Court's holding must be read in light of its explicit finding that the primary purpose of the statute was to question potential witnesses, not potential culprits. *See supra* note 98.

[105] *See, e.g.*, Gerstein v. Pugh, 420 U.S. 103, 112 (1975) (noting that probable cause requirement seeks "to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime" and stating that "[t]o allow less would be to leave law-abiding citizens at the mercy of the officers' whim or caprice" (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949))).

[106] *Lidster*, 540 U.S. at 427.

[107] For more regarding the intrusiveness of DNA collection, see Part I.B.2, *supra*.

state's interest is *weaker* if it is not investigating a suspected present or past crime.[108] Suppose police were to search private residences without a warrant, recording distinctive garments or photographing potential weapons that could identify or incriminate current occupants in the event of future crimes. If gathering information that might be of use in future crimes were a valid special need, such a practice would be subject to a balancing test. In reality, however, such searches would clearly be per se unreasonable, as police action is viewed less favorably, not more, if it is not linked to any past or present crime.

The purpose of storing information relevant to potential future crimes is not a special need but simply the general purpose of law enforcement, weakened by being at a purely speculative stage. As criminal DNA database statutes primarily serve this purpose, they cannot be justified under the special needs rationale.

B. The Diminished Privacy Interest Rationale

The Third, Fourth, Fifth, Eighth, Ninth, and Eleventh Circuits have upheld criminal DNA database statutes under what could be called the "diminished privacy interest" rationale.[109] Under this exception to the warrant requirement, warrantless and suspicionless searches may be analyzed for reasonableness by balancing the individual's interest against the state's so long as the individual's privacy interest is judicially determined to be diminished.[110] A diminished privacy interest is weighed as a factor in this balancing test as well as

---

[108] Attempts, conspiracies, and criminal solicitation are criminalized separately, and are thus present crimes, not future crimes. *See, e.g.*, MODEL PENAL CODE § 5.01 (1962) (criminal attempt); *id.* § 5.02 (criminal solicitation); *id.* § 5.03 (criminal conspiracy).

[109] United States v. Kraklio, 451 F.3d 922, 924–25 (8th Cir. 2006); United States v. Sczubelek, 402 F.3d 175, 184 (3d Cir. 2005), *cert. denied*, 126 S. Ct. 2930 (2006); Padgett v. Donald, 401 F.3d 1273, 1280 (11th Cir. 2005), *cert. denied sub nom.* Boulineau v. Donald, 126 S. Ct. 352 (2005); United States v. Kincade, 379 F.3d 813, 832 (9th Cir. 2004) (en banc), *cert. denied*, 544 U.S. 924 (2005); Groceman v. Dep't of Justice, 354 F.3d 411, 413 (5th Cir. 2004); Jones v. Murray, 962 F.2d 302, 306–07 (4th Cir. 1992), *cert. denied*, 506 U.S. 977 (1992). Courts refer to this approach as a general balancing test, *e.g.*, Nicholas v. Goord, 430 F.3d 652, 659 (2d Cir. 2005), *cert. denied*, 2006 WL 2094481 (U.S. Oct. 10, 2006) (No. 06-131), or a totality of the circumstances test, *e.g.*, *Sczubelek*, 402 F.2d at 184. However, the special needs rationale involves a balancing test as well, *see supra* note 84, rendering the courts' terminology ambiguous. The search target's diminished privacy interest plays a role analogous to a special need, in that both the diminished interest and the special need serve as triggers for a subsequent general balancing test. I refer to each rationale by its respective triggering condition, and thus call this the diminished privacy interest rationale.

[110] Courts generally refer to a diminished privacy interest as a diminished or reduced reasonable expectation of privacy. *E.g.*, Samson v. California, 126 S. Ct. 2193, 2197 (2006). However, the reference to expectations, even reasonable expectations, is misleading. What the courts are talking about has nothing to do with what an individual subjectively expects, but reflects instead a judicial conclusion that society is not prepared to recognize as reasonable the prospect of the individual enjoying full privacy interests in the relevant area. *See,*

in the special needs balancing test.[111] What is unique about the diminished privacy interest rationale is that it treats a diminished privacy interest not only as a factor in a balancing test but also as the trigger allowing the balancing test to be used at all.

This exception has its roots in *United States v. Knights*,[112] where the Supreme Court used a general balancing test to uphold a warrantless search of a probationer's house for contraband based only on reasonable suspicion, instead of probable cause.[113] The Court declined to use the special needs rationale in that case because it found that the probation condition had two purposes—rehabilitation and the deterrence of recidivism—of which only the former was a special need.[114]

In *United States v. Kincade*,[115] a plurality of Ninth Circuit judges sitting en banc relied on *Knights* to uphold a DNA database statute. The plurality concluded that the factor triggering *Knights*'s general balancing test was the probationer's diminished privacy interest,[116] even though the *Knights* Court had not made that clear.[117] The Ninth Circuit plurality found that the supervised releasee challenging the DNA statute also had a diminished privacy interest and proceeded to apply the balancing test.[118] The *Kincade* plurality, like every other

e.g., Amsterdam, *supra* note 11, at 384 ("An actual, subjective expectation of privacy obviously has no place in . . . a theory of what the fourth amendment protects.").

111 *See, e.g.*, *Kincade*, 379 F.3d at 838–39 (plurality opinion) (weighing governmental interests, intrusion on privacy, and convicts' diminished privacy interests).

112 534 U.S. 112 (2001).

113 *Id.* at 121 ("We hold that the balance of these considerations requires no more than reasonable suspicion to conduct a search of this probationer's house.").

114 The Court explained:

> The State has a dual concern with a probationer. On the one hand is the hope that he will successfully complete probation and be integrated back into the community. On the other is the concern, quite justified, that he will be more likely to engage in criminal conduct than an ordinary member of the community. The view of the Court of Appeals in this case would require the State to shut its eyes to the latter concern and concentrate only on the former. But we hold that the Fourth Amendment does not put the State to such a choice.

Id. at 120–21.

115 379 F.3d 813.

116 *Id.* at 832 (plurality opinion) (distinguishing *Knights* from *Edmond* and *Ferguson* by invoking probationers' diminished privacy interests).

117 *Knights*, 534 U.S. at 118 ("[W]e conclude that the search of Knights was reasonable under our general Fourth Amendment approach of 'examining the totality of the circumstances,' with the probation search condition being a salient circumstance." (quoting Ohio v. Robinette, 519 U.S. 33, 39 (1996))). *Robinette* dealt with the validity of a stopped defendant's consent to a search, 519 U.S. at 36, and thus does *not* reflect the Court's general approach to when it is proper to search or seize a nonconsenting suspect, *see supra* notes 77–80 and accompanying text (describing warrant requirement and exceptions). Still, *Kincade*'s assumption that the presence of a diminished privacy interest triggered the balancing test is a plausible inference from *Knights*'s mention of the individual's conditions of probation as "salient." *Knights*, 534 U.S. at 118.

118 *Kincade*, 379 F.3d at 832–33 (plurality opinion).

circuit to employ the diminished privacy interest rationale, concluded that the balancing test favored the state. It thus found the challenged DNA database statute constitutional.[119]

The use of a balancing test without a special need has some doctrinal support, but it is not a principled methodology. In *Samson v. California*, the Supreme Court recently extended *Knights* to allow suspicionless searches of parolees, though it was similarly oblique in its explanation of what triggered the balancing test.[120] Assuming that the circuits are correct in concluding that what triggers the use of the test in *Samson* and *Knights* is the search target's diminished privacy interest, there are still two problems with this approach.

First, there is no clear rule for determining when an individual's privacy interests are sufficiently diminished to invoke a balancing test.[121] Even if there were a consistent standard for finding a diminished privacy interest, not all cases in which courts find diminished privacy interests trigger balancing tests as opposed to categorical rules.[122] Evidently a diminished privacy interest is a conclusory

[119] *Id.* at 839; *accord* United States v. Kraklio, 451 F.3d 922, 924–25 (8th Cir. 2006); United States v. Sczubelek, 402 F.3d 175, 187 (3d Cir. 2005), *cert. denied*, 126 S. Ct. 2930 (2006); Padgett v. Donald, 401 F.3d 1273, 1280 (11th Cir. 2005), *cert. denied sub nom.* Boulineau v. Donald, 126 S. Ct. 352 (2005); Groceman v. Dep't of Justice, 354 F.3d 411, 413–14 (5th Cir. 2004); Jones v. Murray, 962 F.2d 302, 308 (4th Cir. 1992), *cert. denied*, 506 U.S. 977 (1992).

[120] Samson v. California, 126 S. Ct. 2193, 2200–01 (2006) (concluding reasonable suspicion requirement "would give parolees greater opportunity to anticipate searches and conceal criminality"). *Samson* again called the balancing test its "general Fourth Amendment approach" without reference to privacy interests or special needs. *Id.* at 2197 (quoting *Knights*, 534 U.S. at 118); *see supra* note 117 (noting this is not Court's general approach to such cases). However, it did state that the question it was answering (in the affirmative) was "whether a condition of release can so diminish or eliminate a released prisoner's reasonable expectation of privacy" as to justify that releasee's suspicionless search. *Samson*, 126 S. Ct. at 2196; *see also supra* note 110 (noting that "reasonable expectation of privacy" refers not to actual expectation but to privacy interest).

[121] When courts offer an argument for their conclusion that an individual's privacy interest is diminished, it usually consists of an analogy to a type of privacy burden that individual already bears. However, there is no clear reason why the existence of one privacy burden justifies the imposition of some additional privacy burden. Therefore, while it is true that parolees and prisoners are subject to some searches that would be impermissible if applied to members of the populace, *see, e.g.*, Hudson v. Palmer, 468 U.S. 517, 527–29 (1984) ("A right of privacy in traditional Fourth Amendment terms is fundamentally incompatible with the close and continual surveillance of inmates and their cells required to ensure institutional security and internal order."), it is unclear why this gives them a diminished privacy interest that justifies their being subject to *other* searches.

[122] For example, persons have diminished privacy interests with respect to property they bring into cars, Wyoming v. Houghton, 526 U.S. 295, 303 (1999), but a search of luggage in the trunk of a car still requires probable cause (though not a warrant) without any balancing analysis being conducted, *see* United States v. Ross, 456 U.S. 798, 809 (1982) (holding exception to warrant requirement "applies only to searches of vehicles that are supported by probable cause").

finding, and its use to justify an exception to the warrant requirement is thus circular. We should reject a theory of the Fourth Amendment that allows suspicionless searches to be undertaken based only on the ipse dixit of a court's decision that an individual's privacy interests are not at some hypothetical zenith.

Second, criminal DNA database statutes authorize retention of DNA profiles and samples long after the search target has left the criminal justice system and had her full privacy interest restored.[123] Since the burden on privacy endures as long as the record is maintained in the government's database,[124] there is no reason for the government to be able to "tag" someone while he is subject to a diminished privacy interest and use this temporary diminution to burden his privacy for life.[125] While the government does not have to

[123] Some courts claim that those convicted of any crime have diminished privacy interests for life. *Sczubelek*, 402 F.3d at 184–85 ("After his conviction of a felony, [defendant's] identity became a matter of compelling interest to the government . . . ."); *Kincade*, 379 F.3d at 837 (plurality opinion) ("[O]nce a person is convicted [of a predicate offense under the federal DNA statute], his identity has become a matter of state interest and he has lost any legitimate expectation of privacy in the identifying information derived from blood sampling." (quoting Rise v. Oregon, 59 F.3d 1556, 1560 (9th Cir. 1995))); Green v. Berge, 354 F.3d 675, 680 (7th Cir. 2004) (Easterbrook, J., concurring) ("Established criminality may be the basis of legal obligations that differ from those of the general population." (citing McKune v. Lile, 536 U.S. 24, 36 (2004))). But this is a conclusory assertion, *supra* notes 121–22 and accompanying text, and quite inconsistent with current practice. There is no "ex-convict exception" to the warrant requirement; when police wish to search the house of an ex-convict, they are still required to seek a warrant. *See* Kaye & Smith, *supra* note 13, at 417–21 (arguing that theory of permanent diminution of privacy is "a conclusion in search of an argument" and inconsistent with Supreme Court precedent); Antoine McNamara, Note, *The "Special Needs" of Prison, Probation, and Parole*, 82 N.Y.U. L. REV. 209 (2007) (arguing that convicts do not forfeit Fourth Amendment rights by virtue of their status alone). Indeed, even in *Samson*, when discussing the parolees' diminished privacy interests, the Court invoked their supervision by the state, not any lifelong forfeiture of rights by virtue of conviction. 126 S. Ct. at 2199–2201 (agreeing with California legislature that requirement of individualized suspicion "would undermine the State's ability to effectively supervise parolees and protect the public from criminal acts by reoffenders").

[124] *See supra* Part I.B.2 (describing burdens of privacy borne by DNA donors while their profiles remain in database).

[125] Of course, this is how fingerprints are treated. *See, e.g.*, Hammons v. Scott, 423 F. Supp. 618, 623–24 (N.D. Cal. 1976) (finding no constitutional violation in maintenance of arrest records, including fingerprints, even when arrest did not result in conviction). However, fingerprinting alone, independent of the detention needed to procure the fingerprints, is not considered a search under the Fourth Amendment. *See* Davis v. Mississippi, 394 U.S. 721, 724–28 (1969) (analyzing constitutionality of compelled fingerprinting solely by reference to lawfulness of detention during which fingerprints were obtained); *Kincade*, 379 F.3d at 874 (Kozinski, J., dissenting) (noting that practice of fingerprinting predated modern analysis of what tactics constitute searches, allowing fingerprinting to remain unregulated by Fourth Amendment). Admittedly, it does seem somewhat arbitrary that there are no restrictions on the future uses of fingerprints just because they are obtained by a process that does not require submission of internal body matter and thus does not constitute a search. However, this arbitrariness is an inevitable byproduct of the traditional

dispose of information that it obtains through lawful methods, a temporary diminution in privacy should not be the justification for an otherwise unlawful permanent burden on privacy.[126]

C. A General Balancing Test?

Neither the special needs rationale nor the diminished privacy interest rationale justifies criminal DNA databases, even those with the privacy safeguards I suggest. One might be tempted simply to uphold appropriately safeguarded DNA databases as reasonable under the totality of the circumstances. Perhaps, that is, the circuits erred in concluding that *Samson* and *Knights* required a diminished privacy interest before triggering a balancing test. *Samson* and *Knights* referred to their balancing tests as applications of a "general Fourth Amendment approach."[127] Furthermore, the Fourth Amendment only requires reasonableness. Why not evaluate a search's reasonableness simply by weighing the state's interest against the intrusion on individual privacy?

This approach has intuitive appeal, but balancing tests are too subjective,[128] and too vulnerable to slippery slopes,[129] to undergird the type of right to privacy that the Fourth Amendment requires.[130] If

bright-line rules that characterize Fourth Amendment jurisprudence. *See* Amsterdam, *supra* note 11, at 395 ("[M]aintenance of the traditional monolithic model of the fourth amendment makes decisions regarding the boundaries of its coverage excruciatingly difficult."). Despite this drawback, such a bright-line approach is necessary to prevent the Fourth Amendment from collapsing into pure subjectivity. *See infra* notes 128–31 and accompanying text.

126 At least, not if suspicionless searches are to remain a "closely guarded category." Chandler v. Miller, 520 U.S. 305, 309 (1997).

127 *See supra* notes 117, 120.

128 *See, e.g.*, Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173, 1184–1207 (1988) (arguing that Fourth Amendment balancing tests are subjective and inappropriately favor government).

129 *See, e.g.*, Amsterdam, *supra* note 11, at 393–94 (noting that sliding scale approach would "produce more slide than scale"). Where the justification for judicial outcome A is sufficiently vague, as is the case in a totality-of-the-circumstances test, it is impossible to be sure that it will not, in the minds of future judges, also justify judicial outcome B. *See* Volokh, *supra* note 42, at 1074–75 (providing example of this sort of slippery slope). Additionally, once judges decide that a certain balance is justifiable, rationally ignorant actors may assume that this decision is well-reasoned and be more likely to extend this reasoning to similar cases. *See id.* at 1079–80 (describing effect of "is-ought heuristic" in creating attitude-altering slippery slopes). This is especially likely if the expansion occurs gradually. *See id.* at 1105–14 (arguing that inattention to small changes leads to slippery slopes); *id.* at 1114 ("Some small changes can happen simply because judges are faithfully trying to apply a vague rule.").

130 *See, e.g.*, Amsterdam, *supra* note 11, at 394 ("If there are no fairly clear rules telling the policeman what he may and may not do, courts are seldom going to say that what he did was unreasonable." (internal citation omitted)); Strossen, *supra* note 128, at 1184 ("The

judges were competent simply to weigh the competing interests for each search and determine whether that search was reasonable, there would be no need for a uniform warrant requirement in the first place.[131]

Perhaps, then, it would be best to create a category for reasonable criminal DNA databases as a new exception to the warrant requirement.[132] Certainly courts have carved out category-specific exceptions in the past.[133] This is the approach that I will attempt in the next Part, but it is important that there be a principled rationale for the exception. If a judge justifies an exception simply by weighing the interests and concluding that they favor a certain type of database, then those who do not share his assessment of the interests will suspect that he is really conducting a case-by-case balancing test after all. How are they to know that he will not propose a new "heinous crime" or "understaffed police department" exception based on his weighing of the interests in *those* cases?

To avoid such arbitrariness, an exception to the warrant requirement must rest on a broader theory of the purposes of having a warrant requirement at all. For this reason the exception I propose in the next Part, rather than being an assertion that certain *types* of searches are reasonable, is an exception to the warrant requirement that applies when certain reliable *methods* are available to determine what searches are reasonable.

effect of relegating fundamental rights to the inevitable vicissitudes of individualized, subjective decision making is necessarily to give them little, if any, more judicial protection than would be afforded to interests of a nonconstitutional stature.").

131 *See, e.g.*, Amsterdam, *supra* note 11, at 394–95 (explaining warrant requirement as attempt to avoid perils caused by examination of "the facts and circumstances of each case" (quoting United States v. Rabinowitz, 339 U.S. 56, 63 (1950), *overruled by* Chimel v. California, 395 U.S. 752, 768 (1969))).

132 D.H. Kaye advocates such an approach. Kaye, *Special Needs*, *supra* note 13, at 192–95 (advocating "biometric identification" exception). Kaye's approach appears to be based entirely on the status of DNA databases as involving identification, which is not entirely satisfying. First, identification information is not treated differently than other information in other search contexts, *cf.* Part II.A *supra*, and second, it is unclear why this particular category of search, and not any other category of search, deserves an exception. *See infra* text following note 133.

133 *See, e.g.*, Camara v. Municipal Court, 387 U.S. 523, 534–39 (1967) (creating administrative search exception as precursor to special needs exception); Carroll v. United States, 267 U.S. 132, 149 (1925) (creating automobile exception to warrant requirement).

III
AN ALTERNATIVE JUSTIFICATION FOR CRIMINAL DNA DATABASES

In Part I, I argued that although current DNA databases pose serious risks of abuse, DNA investigation with specific safeguards could ideally be a boon both to law enforcement and civil liberties. In Part II, I argued that existing Fourth Amendment jurisprudence does not provide a principled rationale justifying DNA databases with or without safeguards, and that the subjectivity of balancing tests counsels against simply carving out exceptions to the warrant requirement without an underlying rationale.

It might be natural to conclude from this that a DNA database is simply a good idea forbidden by the Constitution.[134] But it is hard to see how a database with the safeguards I describe would truly be inconsistent with the Fourth Amendment's underlying principle of reasonableness. The fear, then, is not that all databases would be substantively unreasonable, but rather that there is no good way to allow such reasonable searches while screening out unreasonable searches. In this Part, I propose such a method.

A. Universality

The Fourth Amendment prohibits unreasonable searches and seizures, but it is often hard to fashion a rule for deciding which searches are reasonable and which are not. The warrant requirement is the traditional method, but outside of familiar contexts it is not particularly helpful. When searches and seizures such as DNA databases bear novel costs and benefits, courts are ill-equipped to determine what is reasonable and what is not. If the problem is the incapacity of the judiciary to make these determinations on its own, a solution might be to enlist the advice of a body not subject to this incapacity.

In the case of most searches and seizures, there is no such solution. The incapacity of executive officers engaged in the "often competitive enterprise of ferreting out crime" to reliably make such determinations is itself the impetus for the warrant requirement.[135] Moreover, criminal defendants and suspects are not politically well-represented constituencies, leading legislatures to undervalue their

134 Although the Constitution has many attractive features, it surely forbids some desirable outcomes, such as the prospect of a supremely qualified foreign-born citizen serving as president. U.S. CONST. art. II, § 1, cl. 4 ("No Person except a natural born Citizen . . . shall be eligible to the Office of President . . . .").

135 Johnson v. United States, 333 U.S. 10, 14 (1948).

privacy interests.[136] Existing DNA databases are subject to just this problem. Law enforcement officers and legislatures have little incentive to respect the privacy of convicts and arrestees.[137] Consequently, as I argued in Part I, current database statutes fail to provide reasonable safeguards against the risk of abuse.

However, if such a statute imposed the same privacy burden on every member of society, a well-functioning democratic legislature could be more competent than the judiciary in determining whether searches or seizures authorized by the statute are reasonable. Although legislatures have little incentive to respect the privacy of convicts and arrestees, they have tremendous incentive to respect the privacy of their constituencies as a whole. Given a well-functioning political system, a *universal* DNA database—one requiring sample collection from the entire population—would not be enacted, or if enacted would not long survive, if most of the populace was materially dissatisfied with the privacy burdens it imposed. As a result, any statute that passes through such a process is likely to have substantial privacy safeguards, and thus the passage of such a statute can be seen as prima facie evidence of the statute's reasonableness under the Fourth Amendment.

Accordingly, I propose a universality exception to the warrant requirement. It would allow judges to conduct a balancing test to determine a search's reasonableness, provided that (1) the search was conducted pursuant to a statute requiring exactly the same search or seizure to be performed on every member of the public to the same degree and on the same terms, and (2) the statute was produced by a well-functioning democratic political process.

As I argued in Part II, properly understood, the special needs rationale and the diminished privacy interest rationale do not justify existing DNA databases. Since these databases affect only a tiny segment of the population, they would similarly be ineligible for the universality exception. The universality exception would, however, allow universal (statewide or nationwide) criminal DNA databases to be analyzed under a balancing test.

---

136 *See, e.g.*, Donald A. Dripps, Essay, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Accused?*, 44 SYRACUSE L. REV. 1079, 1081 (1993) (arguing that political process undervalues rights of criminal suspects and defendants). *But see* William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 780, 782–83 (2006) (arguing that criminal suspects may be adequately represented in political process, though defendants and convicts certainly are not).

137 *See* Solove, *supra* note 41, at 1116 ("[M]any of the people asserting a right of privacy against government information-gathering are criminals or terrorists, people we do not have a strong desire to protect.").

The inclusion of a balancing test may seem odd given my argument that such tests are not firm foundations for constitutional rights,[138] but in the end courts will always have to evaluate the costs and benefits of any search or seizure if they are not to abdicate their responsibility to uphold the Constitution. One might be tempted to conclude that universal searches that have passed through the political process are so certain to be reasonable that further judicial inquiry is unnecessary. This, though, would be a mistake. While it is likely that the political process would weed out universal search regimes that imposed burdens unreasonable in comparison to their benefits, it is by no means certain. Different subjective valuations of privacy,[139] crisis-induced panic, or simple inattention to the legislature might lead a majority to acquiesce in an unreasonably burdensome search regime. Passage through a well-functioning political process provides strong prima facie evidence of the reasonableness of a universal search regime, but it is not dispositive.

In light of the possibility of unreasonable universal search regimes, the best course is for judges to engage in their own de novo reasonableness inquiry. While the judicial balancing test is not a firm bulwark for fundamental rights, it does present the judiciary's best attempt to evaluate novel cases. Under the universality exception, it can serve as an additional check on unreasonable universal search regimes without threatening to swallow the entire Fourth Amendment.

B. Objections to the Universality Rationale

The most natural objection to the universality exception to the warrant requirement is that it is the role of judges to evaluate constitutional provisions in legal disputes.[140] This may be true,[141] but it is beside the point. While the universality exception draws on political process constitutional theories inspired by the work of John Hart

---

138 *See supra* note 128–131 and accompanying text.

139 If fifty-one percent of the populace does not care about the intrusion caused by DNA collection and forty-nine percent does care, an unduly burdensome database might still pass through the political process. I am indebted for this point to Professor Stephen J. Schulhofer.

140 *E.g.*, W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 638 (1943) ("The very purpose of a Bill of Rights was to withdraw certain subjects from the vicissitudes of political controversy, to place them beyond the reach of majorities and officials and to establish them as legal principles to be applied by the courts.").

141 *But see, e.g.*, LARRY D. KRAMER, THE PEOPLE THEMSELVES 250 (2004) (arguing that Supreme Court, as one branch of government, should not be able to "order the others about with impunity").

Ely,[142] it does not abrogate or limit the judicial role. The requirements of universality and a well-functioning political process are intended to persuade, not to overrule, the courts, who would still conduct an independent balancing test in making their final determination as to the constitutionality of a particular enactment.

One might object that legislatures are not more competent than the judiciary even when forced to internalize the costs of their laws.[143] For example, actual legislatures might simply be insufficiently representative to make decisions worthy of respect, even when passing laws that affect all constituents.[144] However, if that were true, the universality exception would not apply. Part of employing the universality exception entails making a judicial determination that the political process is functioning well enough that its outputs are deserving of respect.[145]

One might instead object that the exception will swallow the warrant requirement, but this possibility seems unlikely. Virtually no search regime affects everyone equally.[146] Even measures hailed as

142 The seminal work in this vein is Ely's *Democracy and Distrust*, which argues that judicial interpretation of open-textured constitutional provisions should be guided not by any set of substantive values, but only by the purpose of facilitating the functioning of the political process. JOHN HART ELY, DEMOCRACY AND DISTRUST 87–104 (1980). Political process theories have rarely been applied to the Fourth Amendment. For perhaps the most comprehensive attempt to do so, see Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 92–100 (1988).

143 One form of this objection states that not all reasons that might motivate voters are grounds for depriving citizens of their liberty. *See, e.g.*, Ronald Dworkin, *The Forum of Principle*, 56 N.Y.U. L. REV. 469, 512–16 (1981) (arguing judicial review can be based on view that Constitution includes "rights that legislation not be enacted for certain reasons"). This position is controversial in itself. *See generally* ELY, *supra* note 142 (rejecting view that judges should impose values on democratic nations). But even those who subscribe to it, as I do, should realize that the reasons motivating generally applicable crime control laws are unquestionably the type of reasons that justify depriving citizens of liberty. Decisions about what searches are reasonable are decisions about how to balance ordinary harms and benefits. Seeking to ensure security and privacy for its citizens is a governmental endeavor supported by democratically legitimate reasons, unlike, say, regulating consensual intimate behavior between adults.

144 This view asserts, in essence, that our legislatures are so undemocratic even when internalizing the costs of their legislation that liberal values are always better protected by an oligarchic judiciary.

145 One might doubt the ability of courts to inquire into the functioning of the political process. This worry, however, applies with equal force to all political process theories of the Constitution, not merely the universality exception. *Cf.* ELY, *supra* note 142, at 135–79 (making similar judicial inquiry central to theory of Equal Protection Clause).

146 This is no doubt part of why the political process, such a central feature in constitutional theory, is such a tangential part of Fourth Amendment jurisprudence. *See supra* note 142.

broadly applicable,[147] or justified as the product of a representative political process,[148] are not truly equal in this way.[149] Some of these searches may be allowed, but only if they also further a non–law enforcement special need: Sobriety checkpoints burden a wide range of people[150] but not everyone equally, and it is entirely at the police department's discretion where to deploy them.[151] In contrast, a universal DNA database would apply equally to everyone,[152] and it is thus sufficiently more likely to be reasonable than an ordinary search that a balancing test could be conducted even in the absence of a special need. Indeed, the political checks facing a universal search regime surely constitute a more reliable indicator of the palatability of the search, and thus a better trigger for the balancing test, than a judicial finding of a special need.[153]

C. Objections to a Universal DNA Database

The universality rationale would require a criminal DNA database to be universally applicable. It is natural to suppose that if current DNA databases are bad, extending them to everyone would be worse. However, this concern fails to take seriously the advantages of a universal database. First, each suspect identified through a database match represents a shortcut past a number of intrusive and

147 *See, e.g.*, Wasserstrom & Seidman, *supra* note 142, at 95 (predicting that roadblocks would be acceptable under political process theory of Fourth Amendment due to their broad impact).

148 Dan M. Kahan & Tracey L. Meares, *The Coming Crisis of Criminal Procedure*, 86 GEO. L.J. 1153, 1171–76 (1998) (advocating constitutionality of discretionary community policing searches when community being burdened is represented in political process); Tracey L. Meares & Dan M. Kahan, *The Wages of Antiquated Procedural Thinking: A Critique of* Chicago v. Morales, 1998 U. CHI. LEGAL F. 197, 209–11 (similar).

149 Albert W. Alschuler & Stephen J. Schulhofer, *Antiquated Procedures or Bedrock Rights? A Reply to Meares and Kahan*, 1998 U. CHI. LEGAL F. 215, 240–43 (arguing that definition of "community" used by Kahan and Meares is manipulable and unhelpful).

150 *See supra* note 147.

151 Perhaps due in part to this lack of true universality, such checkpoints are only constitutional if they serve a special need. *Compare* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (upholding suspicionless highway checkpoints as serving special need of removing drunk drivers from road), *with* City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000) (prohibiting suspicionless highway checkpoints when law enforcement is primary purpose).

152 DNA collection affects the guilty more than the innocent, but this is a virtue, not a vice. What is significant is that it subjects everyone to the exact same search. The easiest way to achieve universal coverage would require DNA collection at birth. This would of course take a great deal of time to phase in, and could potentially be supplemented by DNA collection during hospital visits or other relatively convenient times.

153 *Cf.* ELY, *supra* note 142, at 183 ("[C]onstitutional law appropriately exists for those situations where representative government cannot be trusted, not those where we know it can.").

error-prone investigative techniques.[154] Second, a universal database would represent all racial groups proportionately, in contrast to a database created by arrest or conviction.[155] Third, the DNA database would have passed through the political process, and the universal burdens would likely lead to the adoption of significant safeguards.

There is an additional worry, however, that a universal DNA database would be a burden on collective privacy in a way that a more limited one would not.[156] Indeed, the fear of a broader database has lurked in the background of the debate over existing laws. Few of the dissents to the decisions upholding the statutes have focused on the reasonableness of taking DNA from the convicted offenders at issue, instead concentrating on the likelihood of future expansion to other groups.[157]

One might worry that everyone's presence in a database would be one step towards totalitarianism in making it easier for the government to identify and arrest dissidents.[158] If the database were anonymous, however, it could not be used for roundups unconnected to

154 *See supra* Part I.B.1. There is good reason to believe that expanding the database to the population would vastly increase the number of hits even though the database would include many individuals not known to be criminals. *See, e.g.*, Kaye & Smith, *supra* note 13, at 451–52 (noting that forty-four percent of felony arrestees have no prior felony arrests, and approximately one-third have no prior arrests at all (citing BRIAN A. REAVES, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, PUBL'N NO. NCJ-167234, FELONY DEFENDANTS IN LARGE URBAN COUNTIES, 1994, EXECUTIVE SUMMARY, at 2 (1998))).

155 Kaye & Smith, *supra* note 13, at 452–59 (noting overrepresentation of minorities in database containing convicts and arrestees and arguing that population-wide database would alleviate racial tensions).

156 Daniel J. Solove notes that focusing only on the privacy rights of each individual, especially if the individuals in question are "criminals or terrorists, people we do not have a strong desire to protect," can lead to an undervaluation of privacy. Solove, *supra* note 41, at 1116 ("Privacy is not merely a right possessed by individuals, but is a form of freedom built into the social structure. It is thus an issue about the common good as much as it is about individual rights.").

157 *See, e.g.*, United States v. Kincade, 379 F.3d 813, 843 (9th Cir. 2004) (en banc), *cert. denied*, 544 U.S. 924 (2005) (Reinhardt, J., dissenting) (stating that society "would be lucky indeed" if rationale authorizing DNA statutes confined collection to convicted offenders); *id.* at 872 (Kozinski, J., dissenting) ("Which brings us to the people we really need to worry about [being subject to DNA sampling], namely you and me."); *id.* at 876 (Hawkins, J., dissenting) ("In a world unrestrained by our Fourth Amendment, every citizen, convicted or not, might be forced to supply a DNA sample."). *But see* United States v. Sczubelek, 402 F.3d 175, 204 (3d Cir. 2005), *cert. denied*, 126 S. Ct. 2930 (2006) (McKee, J., dissenting) ("I do not concede that the DNA Act would be a reasonable intrusion under the Fourth Amendment if Congress had restricted the information to the term of an individual's supervision under the criminal justice system.").

158 *See supra* note 42 and accompanying text.

crimes and would be less dangerous in this regard than a phone directory.[159]

Perhaps the sheer increase in law enforcement effectiveness caused by a universal database, even if the data is not abused, would nevertheless foster an unwholesome culture of obedience.[160] It might be true that American-style democracy requires the possibility of at least some illegality to promote appropriately adversarial and dissenting norms. However, society is nowhere near the point where it needs to start worrying that law enforcement is too accurate.

And while there may be some risk of development of unhealthy norms, it is not at all clear that this is the direction the slippery slope will run. Not all chain reactions are evil. A world where violent crime perpetrators are in almost all cases quickly identified might foster positive norms. Citizens might gain increased respect for the justice system if it is less prone falsely to convict minorities of violent crimes, and this increased trust could lead to greater civic involvement.[161] Or if violent crime is significantly deterred by swift identification of the perpetrators, the decline in its incidence could reduce the public's fear of all crime.[162] Perhaps with fewer lurid spectacles of murders and rapes, the public would be less prone to view crime as out of control, and would moderate its attitudes toward other crimes. This is pure speculation, but so is the fear that accurate law enforcement, achieved without revealing private details of people's lives, would lead to totalitarianism.

---

159 The possibility of national security–related executive disobedience of a statutory command to keep the master list separated from the profile database does increase this risk somewhat, but banning a technology for fear that no law can restrain an executive from misusing it is extreme indeed. *See supra* note 67.

160 That is, the fear of a search technique is not merely that it may have too many false positives; it is also that it may have too few false negatives. Imagine a world where an omniscient robot showed up whenever any crime was committed, no matter how small, and politely but firmly whisked the criminal away. Even if the robot paid no attention to non-criminal behavior and never arrested an innocent person, and even if sentencing was still in the hands of human authorities, one nonetheless imagines that people in that world would wind up being too docile and submissive to allow for a vigorous and thriving democracy.

161 *See* Kaye & Smith, *supra* note 13, at 458 (noting that universal DNA database could help counteract perception of racism in criminal investigation).

162 Some scholars suggest that the phenomenon of overcriminalization is driven by voter responses to lurid media reports of crime. *See, e.g.*, Rachel E. Barkow, *Administering Crime*, 52 UCLA L. REV. 715, 748–49 (2005) ("Cognitive psychology teaches that when voters think of crime and sentencing, they tend to think of examples of crimes that are most salient. . . . [T]he most heinous crimes that grab headlines tend to come to mind when voters think about which sentences are appropriate . . . ."). If this is so, reducing the incidence of the most brutal crimes could help lessen the public's fear of all crime.

CONCLUSION

Criminal DNA databases represent a new technology raising both hopes of more efficient and accurate law enforcement, and fears of abuse and the erosion of privacy. Rather than stretching existing exceptions to the warrant requirement that do not fit criminal DNA databases, courts should take the difficulty of weighing these costs and benefits to heart. They should reserve the special needs rationale for those statutes that serve a genuine special need, and if they use the conclusory diminished privacy interest rationale, they should at least restrict it to privacy burdens applied while the individual's privacy is diminished.

Courts might be more willing to hold the line on these existing doctrines if they did not fear that doing so would foreclose the possibility of ever allowing DNA database technology. If they recognized that universal DNA databases represent one of the few feasible technologies whose reasonableness can be reliably assessed by a legislature, they might be willing to allow them under the universality exception I have outlined. Perhaps no universal database could pass such political process. But any such database that does will have been found reasonable by a process far more reliable than any extant doctrine, and it will almost certainly have better privacy safeguards than any DNA database that exists today.