University of Cincinnati Law Review

Volume 79 | Issue 4 Article 1

October 2011

APPLYING THE FOURTH AMENDMENT WHEN DNA COLLECTED FOR ONE PURPOSE IS TESTED FOR ANOTHER

Kelly Lowenberg

APPLYING THE FOURTH AMENDMENT WHEN DNA COLLECTED FOR ONE PURPOSE IS TESTED FOR ANOTHER

*Kelly Lowenberg**

Deoxyribonucleic acid (DNA) contains sensitive information about a person's identity, family, and medical risks. As our understanding of genetics improves, DNA that was originally collected by the government for one purpose is becoming useful for other purposes. Some states are now testing DNA originally collected for identification or medical screening for other purposes, including research and determining whether two people are related. Once the government has taken and tested your DNA, what else can the government reasonably do with it? While others have discussed how the Fourth Amendment limits the initial DNA collection and testing, this Article is the first to examine how the Fourth Amendment applies when these DNA samples are tested for new information.

Because DNA contains a vast amount of information in a microscopic space, rules that traditionally restrict government conduct might be insufficient to establish appropriate limits on how DNA can be analyzed. Drawing on computer-search law in which courts address similar problems, this Article proposes that the Fourth Amendment be applied to focus on what information has been exposed rather than whether a physical zone has been penetrated. This approach would require a warrant or an applicable warrant exception before a DNA sample could be retested for additional genetic information. Applying the Fourth Amendment to DNA testing in this manner is doctrinally supported and strikes the best balance between allowing the government to analyze stored DNA for new purposes when necessary and protecting genetic information from being unreasonably revealed.

* The author is currently serving as a law clerk for the Honorable Edward J. Davila. While writing this Article, she was a fellow at the Stanford Law School Center for Law and the Biosciences.

For valuable conversations and criticisms, I am grateful to Hank Greely, Robert Weisberg, Elizabeth Joh, Alex Pollen, Dov Fox, Ryan Calo, Brenda Simon, Tim Tatarka, Zac Cox, EunHae Park, Dmitry Karshtedt, Alyson Yamada, and Elizabeth Greisman. Thanks also to the staff of The University of Cincinnati Law Review for outstanding editorial support.

INTRODUCTION

The Grim Sleeper, a serial killer, was arrested decades after his first murder, with the aid of a new deoxyribonucleic acid (DNA) forensic technique called familial DNA searching.[1] Police had compared DNA found at crime scenes with DNA of known convicts stored in a database, but no complete matches were found. In the past, that would have been a dead end; however, by performing additional testing on stored DNA samples that partially matched the killer, the investigators established that the killer was closely related to a convicted felon[2] and used this information to finally close a decades-old case. The utility of additional DNA testing in capturing the Grim Sleeper suggests that law enforcement may be well served by exploring additional information

1. Maura Dolan et al., *DNA Leads to Arrest in Serial Case*, L.A. TIMES, July 8, 2010, at A1.
2. See discussion of familial searching, *infra* at p. 1295.

contained in DNA beyond a handful of identity markers.

The government can lawfully collect, analyze, and retain DNA from many groups of people—convicts, arrestees, military personnel, suspects, crime victims, and newborn babies. This collection and initial analysis must pass Fourth Amendment muster, but the law is not clear on whether these DNA samples, once analyzed, can be analyzed a second or a third time.

Familial searching is only one example of the many additional tests that might be conducted on DNA. DNA contains information that can be used to establish our identities and genealogies as well as to predict phenotypic traits like disease risk. Revealing genetic information can have criminal, financial, and psychological consequences for an individual. But this information can also serve important government interests. Can DNA taken from newborns be tested for criminal identification purposes? Could DNA taken from crime victims be tested to establish paternity? Can these stored DNA samples be tested for genetic medical research? Does the Fourth Amendment limit what the government can search for in stored and partially analyzed DNA?

Fourth Amendment law regarding searches of DNA and other information-rich materials is not very developed. The best indicator of how courts will apply the Fourth Amendment to regulate additional DNA testing is how they have dealt with similar issues in searches of computers. Like DNA, computers contain a large amount of information in a very small space and all that raw material must be seized because relevant information cannot be separated from irrelevant information at the site of the search.

The Fourth Amendment has traditionally focused on whether the government may penetrate the physical boundaries of a particular space—enter a house or open a container. Courts have strained to analogize between the physical boundaries of a container and the physical disks in a computer. But this analogy comes apart when applied to DNA and would leave sensitive genetic information contained in DNA specimens, already tested for one purpose, completely unprotected. Rather, emerging Fourth Amendment law that focuses on the content of what is revealed rather than simply the form of the search is better suited to limit genetic testing.

Part I of this Article provides background on DNA and on relevant Fourth Amendment law. Part II discusses problems with limiting the scope of a DNA search merely by focusing on the collection of DNA. Part III draws on computer-search law to evaluate different applications of Fourth Amendment law to an information-rich context and proposes the most suitable approach to regulating DNA analysis.

By limiting the zone of a DNA search to the information that is exposed to the analyst, privacy interests in unrevealed genetic information will be preserved. Thus, the Fourth Amendment would require a warrant or an applicable warrant exception before a DNA sample can be retested for additional genetic information. This approach would allow the government to analyze stored DNA for new purposes when necessary, such as catching the next Grim Sleeper and would also protect genetic information from being unreasonably revealed.

I. BACKGROUND ON DNA AND THE FOURTH AMENDMENT

Before analyzing how the Fourth Amendment applies to these DNA samples and what this indicates about the direction of the Fourth Amendment, this first subsection introduces the basic facts of DNA and how it is currently analyzed. Additionally, this Part will review how DNA collection has fit into the Fourth Amendment framework, and where the courts' involvement has ended and DNA testing by the government has continued.

A. Background on DNA Analysis

DNA is an information-rich material contained in every cell in our bodies. DNA can be collected from a person by swabbing the inside of the person's cheek or drawing blood, and the DNA in the nuclei of the cells in the cheek swab or blood sample can be isolated. DNA is also contained in each cell's mitochondria, but forensic testing is more commonly conducted on nuclear DNA. Each person's DNA contains two sets of twenty-three chromosomes, each set containing over 3 billion nucleotide bases.[3] One set of chromosomes is inherited from one's mother, and one set from one's father. Some portions of the DNA, such as genes, code for proteins, and other portions control expression of those genes. Still other portions, as far as can be determined, do neither and do not indicate anything about how the person is predisposed to look or behave. The variation in DNA contains information about a person's identity, genealogy, and phenotype.

3. LISTER HILL NAT'L CTR. FOR BIOMEDICAL COMMC'NS, DEP'T OF HEALTH & HUMAN SERVS., GENETICS HOME REFERENCE: HANDBOOK 9, 46 (2011), Human Genome Reference, *available at* http://ghr.nlm.nih.gov/handbook.pdf.

1. Identity

Unless a person has an identical twin, DNA can be used as a unique identifier of a person. A perfect match between two samples of DNA indicates that both samples came from the same person. Only a portion of DNA needs to be tested to obtain enough information to affirmatively link a DNA sample to a single person.

The most common form of DNA analysis used to match samples and test for identification in forensic laboratories worldwide analyzes only certain non-coding and non-regulatory regions of DNA. These particular regions of DNA, known as short tandem repeats or satellite tandem repeats (STRs), contain an abundant number of short strings of nucleotides that are prone to repeating. For example, on one chromosome a particular STR might have a set of four nucleotides that repeat three times: ACCTACCTACCT.[4] The number of times these strings repeat varies between individuals.[5] Each person has two copies, or alleles, of each STR locus, one on a chromosome inherited from each parent.

In the United States, in the 1990s the Federal Bureau of Investigation (FBI) chose thirteen STRs that had a wide range of variation in the population in the number of repeats to be the basis for a DNA identification profile.[6] These have become known as the Combined DNA Index System (CODIS) loci. For the thirteen STRs chosen by the FBI, the repeated sequences are four or five nucleotides in length, and there are five to twenty different common variations on the length of the string of repeats.[7] For example, one of the STR loci used by the FBI consists of repeats of AATG located on the short arm of chromosome eleven.[8] In addition to the core thirteen CODIS markers, the amelogenin genes on both the X and Y chromosome are genotyped to indicate the person's sex.[9] The variability in the twenty-six alleles (two

4. Genetic code consists of four nucleic acid bases: adenine ("A"), thymine ("T"), cytosine ("C") and guanine ("G"). For more information, see *id.* at 9.

5. Bruce Budowle & Angela van Daal, *Forensically Relevant SNP classes*, 44 BIOTECHNIQUES 603, 604 (2008).

6. Nat'l Inst. of Standards & Tech., FBI CODIS Core STR Loci, http://www.cstl.nist.gov/strbase/fbicore.htm (last visited Aug. 6, 2010). *See* John M. Butler, *Genetics and Genomics of Core STR Loci Used in Human Identity Testing*, 51 J. FORENSIC SCI. 253, 253 (2006).

7. Budowle & van Daal, *supra* note 5, at 604.

8. Nat'l Inst. of Standards & Tech., STR Fact Sheet—TH01, http://www.cstl.nist.gov/strbase/str_TH01.htm (last visited Aug. 6, 2010).

9. K.M. Sullivan et al., *A Rapid and Quantitative DNA Sex Test: Fluorescence-Based PCR Analysis of X-Y Homologous Gene Amelogenin*, 15 BIOTECHNIQUES 637 (1993) (explaining that a woman with two X chromosomes will have two versions of the amelogenin gene of the same length, while a man with an X and a Y chromosome will have two amelogenin genes with different lengths).

at each of the thirteen loci) is so great that, apart from identical twins, it is extremely unlikely that any two humans share the same set of alleles.[10]

When a DNA sample is collected, a personal profile is created containing numbers indicating the length of those twenty-six repeats (two strings of repeats at each of the thirteen locations) and then added to local,[11] state, and national databases. The combined system of these databases, the Combined DNA Index System (CODIS), is maintained by the FBI.[12] These databases are used to compare existing DNA profiles to DNA samples found at crime scenes in order to identify the source of the crime scene sample.[13]

2. Genealogy

DNA can also reveal information about a person's genealogy. Taking a historical view, DNA can indicate in what continent or region a person's ancestors lived. A simpler form of genealogical information that is useful forensically is whether two people are related. A partial match between two DNA samples indicates that the two donors have a common genetic lineage. Because of differences in mutation rates and differences between chromosomes, a match between particular DNA regions is more informative of a familial relationship than a match between other regions. For example, a match between DNA regions on the Y chromosome is more indicative of patrilineal ancestry because men have two copies of every chromosome except their Y chromosome, of which each man only has one, inherited directly from his father.

Matching STRs on the Y chromosomes, in conjunction with the thirteen CODIS loci, can provide further information about whether and how closely two men are related through their male ancestors. This

10. The statistical uniqueness of a DNA profile is on the order of one in several hundred quadrillions. For example, in *People v. Robinson*, 224 P.3d 55, 62 (Cal. 2010), *cert. denied*, 131 S. Ct. 72 (2010), the defendant's DNA profile was predicted to be "unique, occurring in approximately 1 in 21 sextillion of the Caucasian population, 1 in 650 quadrillion of the African American population, 1 in 420 sextillion of the Hispanic population."

11. A growing number of local DNA databases are not restricted to criminals. Some include the DNA of victims, suspects, or lab workers. These "rogue databases" are not included in CODIS but "rules about their use by law enforcement agencies are unclear." Ellen Nakashima, *From DNA of Family, a Tool to Make Arrests*, WASH. POST, Apr. 21, 2009, at 2, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/04/20/AR2008042002388.html.

12. FBI, CODIS Brochure, http://www.fbi.gov/hq/lab/html/codisbrochure_text.htm (last visited Aug. 6, 2010).

13. In addition to the convicted offender database, there are also databases for crime scene DNA, for arrestee DNA, for missing persons DNA, for unidentified human remains, and biological relatives of missing persons. *Id.*

Y chromosome genotyping is called Y-STR typing. Y-STR typing is similar to the STR analysis described earlier, except that it uses DNA located at ten additional loci on the Y chromosome. Men who share a common genetic father or paternal grandfather will share the same Y STRs.[14]

Information about whether two people are related can be used to generate leads in a criminal investigation, as in the Grim Sleeper case. The Scientific Working Group on DNA Analysis Methods,[15] a group of forensic scientists that works under the guidance of the FBI, recommends that states conduct Y-STR typing as a standard part of their familial searching programs.[16] At least twelve states recommend or require some additional genetic analysis, usually Y-STR typing, be performed before the identity of a possible relative is disclosed.[17] This extra genotyping is useful because "[a]ny offenders not eliminated by the Y-STR type comparison could be patrilineally related to the true perpetrator and will be candidates for further investigation and consideration as potential genetic relatives of the true perpetrator."[18]

Familial searching need not stop with Y-STRs. After all, focusing on the Y chromosome limits analysis to the paternal line of relatives. If more STR loci were analyzed on the other chromosomes, familial searching would be able to say more about two people's degree of relatedness. At the extreme, all the DNA samples stored by government could be fully sequenced and clustered by similarity. These more extensive methodologies for familial searching would yield information that might catch the next Grim Sleeper, but it would also incidentally reveal a large amount of other genetic information.

3. Phenotype

DNA also contains other personal information beyond these common forensic uses. A person's observable characteristics—such as appearance, health, and behavior—are called the person's phenotype. Phenotype is a result of the interaction between a person's genetics and

14. Press Release, George B. Anderson, Dir., Cal. Dep't of Justice, DNA Partial Match (Crime Scene DNA Profile to Offender) Policy (Apr. 24, 2008), *available at* http://www.aclunc.org/news/press_releases/asset_upload_file504_8577.pdf (codifying Y-STR typing protocol for familial searching).

15. Nat'l Forensic Sci. Tech. Ctr., Scientific Working Group on DNA Analysis Methods, http://www.nfstc.org/pdi/Subject10/pdi_s10_m03_01_d.htm (last visited Apr. 4, 2011).

16. GENETIC INFO. WORK GROUP, MINN. DEPT. OF ADMIN., SEARCHING THE CONVICTED OFFENDER REGISTRY 33 (2008), www.ipad.state.mn.us/docs/geninfo17.pdf.

17. Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751, 796 (2011).

18. Press Release, Anderson, *supra* note 14, at 27.

environment, and it can be partly predicted by DNA testing. Some phenotypic information, like eye color, can be easily observed by looking at a person and is not private. Other phenotypic information, like a predisposition to a genetic disease, may not even be known by the individual herself.

Some genetic correlates of disease are highly predictive. For example, if a person has the nucleotide bases CAG repeated more than thirty-six times at a particular location on the short arm of one of their copies of chromosome four, that person will develop Huntington's disease, a fatal neurological and motor disorder. The number of CAG repeats can also predict how early that person will start to experience symptoms of Huntington's disease. Similarly, other gene mutations are highly predictive of diseases like early-onset Alzheimer's disease or Lynch syndrome, which can lead to many forms of cancer. Other diseases, like hemophilia and Tay-Sachs disease, require a person to have two copies of a disease-linked gene. A person with only one version of the gene will not show symptoms, but could have an affected child if the other parent is also a carrier. In contrast to these rare, highly predictive mutations, there are many common variants that more modestly predict disease risk, for example risk for some kinds of cancer[19] and late-onset Alzheimer's disease.[20]

Research efforts to better understand common genetic variations that increase a person's risk for disease focus on identifying individual nucleotide bases that have been substituted with a different base. These single nucleotide differences between people are called "SNPs" or "single nucleotide polymorphisms." If a SNP is located in a gene or a regulatory region, the SNP itself may cause the increased disease risk.

However, even if a SNP does not cause the difference in disease risk, it may be linked to a genetic variant that does. In those cases, the presence of the SNP will still provide information about a person's disease risk. SNPs can be linked to other gene variants as a result of "linkage disequilibrium." Each time a person produces gametes (sperm or eggs), the person's two sets of chromosomes recombine in different ways—sections of DNA on a pair of chromosomes switch places—and these recombination events create variation. Although many of these

19. *See, e.g.*, D. Ford et al., *Genetic Heterogeneity and Penetrance Analysis of the BRCA1 and BRCA2 Genes in Breast Cancer Families*, 62 AM. J. HUM. GENETICS 676 (1998); J. Kononen et al., *Tissue Microarrays for High-Throughput Molecular Profiling of Tumor Specimens*, 4 NATURE MED. 844 (1998).

20. *See, e.g.*, E.H. Corder et al., *Gene Doses of Apolipoprotein E Type 4 Allele and the Risk of Alzheimer's Disease in Late Onset Families*, 261 SCI. 921, 921–22 (1993) (explaining that APOE has three alleles: APOE-2, APOE-3, and APOE-4, and the risk of Alzheimer's disease increases with the number of APOE-4 alleles).

recombination events may take place over the length of the chromosome, it is less likely that much recombination will occur in any small portion of DNA. As a result, nucleotide bases located close together are likely to travel together. If you know a person has one of those bases, then you can strongly predict that the other base is present as well; these two bases are in linkage disequilibrium. More colloquially, one might say that the SNP travels with the genetic variant that causes the disease.

Major government-sponsored research projects looking for genome-wide associations with disease focus on identifying informative SNPs. Private companies are also conducting research on SNPs and selling their DNA-testing services to people who are interested in learning what their SNPs say about them. SNPs may contain "a wealth of genetic information that can be tapped, since approximately 85% of human variation is derived from SNPs."[21]

In addition to these single nucleotide changes, larger structural variation is increasingly being recognized as abundant and important for phenotype.[22] Some people may have entire regions of DNA repeated or missing. There will be fewer of these structural variants, called copy number variants, than SNPs in any one person's genome, but each variant covers more sequence and may make more substantial contributions to phenotype.

A person's DNA, through SNPs or copy number variants, might also indicate her genetic risk for developing a psychiatric disorder.[23] Researchers are investigating the role of genetics in highly heritable psychiatric disorders, such as alcoholism, schizophrenia, and bipolar disorder. Despite the high heritability of these disorders, few reproducible genetic risk factors have been identified.

Some research is also being done into whether DNA variations are associated with behavior. For example, there is some evidence that certain variations in the region of DNA that controls the production of the neurotransmitter inhibitor MAO-A, when combined with particular environmental stressors, are linked to violent behavior.[24] Our

21. Budowle & van Daal, *supra* note 5, at 604.

22. Gregory M. Cooper et al., *Systematic Assessment of Copy Number Variant Detection Via Genome-Wide SNP Genotyping*, 40 NATURE GENETICS 1199 (2008); *see also* Stephen A. McCarroll, *Copy Number Variation and Human Genome Maps*, 42 NATURE GENETICS 365 (2010).

23. *See, e.g.*, Michael C. O'Donovan, *Genetics of Psychosis; Insights from Views Across the Genome*, 126 HUM. GENETICS 3 (2009) (pointing to likely genetic indicators of schizophrenia and bipolar disorder, but acknowledging that very little of the risk of either disorder can be explained genetically).

24. *See, e.g.*, H.G. Brunner et al., *Abnormal Behavior Associated with a Point Mutation in the Structural Gene for Monoamine Oxidase A*, 262 SCI. 578 (1993); Avshalom Caspi et al., *Role of*

understanding of genetic contributions to behavior is nascent, but behavioral genetics research will continue and may yield new information.

DNA can reveal information about a person's identity, genealogy, and phenotype. Within these larger categories of genetic information is data about a person's ancestry, ethnicity, family relations, and medical risks. Research has already begun on new frontiers of genetics, including psychiatric and behavioral genetics. There are many human traits that cannot currently be well explained by genetics, but our understanding of the information contained in DNA will continue to improve.

B. Applying the Fourth Amendment to DNA Collection

The government is now collecting DNA from an increasingly large number of people. DNA is taken from convicted felons in nearly every state,[25] people arrested for certain offenses in twenty-one states,[26] crime victims, and military personnel[27] to test for identification purposes. In addition to testing for identity, DNA can be taken from suspects of crimes to test for other purposes, like paternity.

Blood samples containing DNA are also taken from newborn babies[28] to test for treatable genetic diseases. This testing requires taking a small amount of blood by pricking the newborn's heel and collecting the blood on paper cards, which, in most states, are destroyed after testing. Newborns who have some detectable disorders, such as phenylketonuria, can be treated to prevent or mitigate the disorder.[29]

Genotype in the Cycle of Violence in Maltreated Children, 297 SCI. 851 (2002); Guang Guo et al., *The VNTR 2 Repeat in MAOA and Delinquent Behavior in Adolescence and Young Adulthood: Associations and MAOA Promoter Activity*, 16 EUR. J. HUM. GENETICS 626 (2008); *see also* Nita Farahany & William Bernet, *Behavioural Genetics in Criminal Cases: Past, Present, and Future*, 2 GENOMICS, SOC'Y & POL'Y 72 (2006); Jill C. Schaefer, *Profiling at the Cellular Level: The Future of the New York State DNA Databanks*, 14 ALB. L.J. SCI. & TECH. 559, 576 (2004) ("Currently a growing number of scientists . . . are looking to the DNA strand as a predictor for criminality.").

25. Nat'l Conference of State Legislatures, State Laws on DNA Data Banks, http://www.ncsl.org/default.aspx?tabid=12737 (last visited July 6, 2011) (listing forty-seven states that collect DNA from all convicted felons).

26. *Id.* (listing twenty-one states that by 2009 had passed laws authorizing DNA samples of certain arrestees).

27. Robert Scherer, *Mandatory Genetic Dogtags and the Fourth Amendment: The Need for a New Post*-Skinner *Test*, 85 GEO. L.J. 2007 (1997).

28. In some states, blood spots are taken from newborn babies without consent of the parents in order to screen for life-threatening medical conditions. The blood spots have been stored and used in research. *See, e.g.*, Emily Ramshaw, *DSHS Turned Over Hundreds of DNA Samples to Feds*, THE TEX. TRIB., Feb. 22, 2010, *available at* http://www.texastribune.org/stories/2010/feb/22/dna-deception/#.

29. Susan Hiraki & Nancy Green, *Newborn Screening for Treatable Genetic Conditions: Past, Present and Future*, 37 OBSTETRICS & GYNECOLOGY CLINICS N. AM. 11 (2010).

In addition to these instances of DNA collection, the police have also collected DNA from skin or saliva cells found on objects an individual has discarded. In these circumstances, the government has argued that there is no search or seizure, of the object or of the individual's DNA, because the person had no privacy interests in the abandoned property.[30] That argument raises interesting questions, but this Article will examine only clear cut, frank government seizures of DNA, where the government requires someone to provide a DNA sample.[31] That kind of direct seizure implicates the right to be free from government intrusion and is clearly a search and seizure.[32]

Government collection of DNA is a search, but it has been found to be a constitutional search under various Fourth Amendment tests. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[33]

The purpose of the Fourth Amendment was to prohibit the government from conducting general, open-ended searches, whereby law enforcement could search any individual for anything at any time.[34]

The Fourth Amendment applies to government action that intrudes upon an individual's reasonable expectation of privacy.[35] The touchstone of whether the government can intrude upon that privacy is "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security."[36] Courts have developed several tests to determine whether a particular search is reasonable. The applicable test depends on the circumstances of the search.

30. Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 865 (2006).

31. In addition to "abandoned" DNA, the scope of this Article also excludes looking at participants in government-funded research whose DNA is tested for additional information not contemplated in the participant's consent.

32. United States v. Kincade, 379 F.3d 813, 821 n.15 (9th Cir. 2004).

33. U.S. CONST. amend. IV.

34. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (explaining that the Fourth Amendment's warrant requirement aims to prevent unnecessary, overly broad searches and arose out of colonists' abhorrence to general warrants that permitted "general, exploratory rummaging in a person's belongings").

35. Katz v. United States, 389 U.S. 347, 361 (1967).

36. Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977) (quoting Terry v. Ohio, 392 U.S. 1, 19 (1968)).

Ordinarily, in order for a search or seizure to be reasonable, the government must obtain a search warrant. The Warrant Clause in the Fourth Amendment requires law enforcement officers to demonstrate to a neutral magistrate that they have probable cause to believe that the search will reveal particular evidence of a crime. As with any other type of evidence, DNA can be collected pursuant to a warrant if police officers demonstrate probable cause to a magistrate that the DNA will be evidence of a crime. DNA warrants have been used to collect DNA from suspects for testing for identification of a crime scene sample or for showing paternity.

A warrant and probable cause are not always necessary for a search to be reasonable. For example, if a person consents to being searched, then nothing else—neither warrant nor probable cause—is necessary. Some DNA collection would not be reasonable but for the consent exception. For example, DNA has been collected by consent from many people during DNA dragnets, in which police canvass areas near crime scenes for possible suspects.[37]

DNA can also be collected under certain circumstances without a warrant because a person's privacy expectation has decreased or the government's need is increased.[38] Searches of certain locations—such as prisons or airport terminals[39]—and groups of people—such as convicted felons—in which an otherwise legitimate expectation of privacy is reduced need only be reasonable based on the totality of the circumstances. The reasonableness of the search is evaluated "by assessing, on the one hand, the degree to which the search intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[40]

Courts have used the totality of the circumstances test to uphold collecting DNA from persons convicted of felonies because felons have

37. Jeffrey S. Grand, *The Blooding of America: Privacy and the DNA Dragnet*, 23 CARDOZO L. REV. 2277, 2297–2302 (2002).

38. In addition to the totality of the circumstances and the special needs frameworks, searches to enforce administrative codes or to accomplish important non-law enforcement goals may not require a warrant. Administrative searches are less likely to permit DNA collection and analysis, so they are beyond the scope of this Article. New York v. Burger, 482 U.S. 691, 702–04 (1987) (noting that warrantless inspection of premises of vehicle-dismantling company is reasonable because it is a "closely regulated" business).

39. Hudson v. Palmer, 468 U.S. 517, 526 (1983) ("[T]he Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell."); United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974) (holding that warrantless airport security searches are reasonable in light of the risk to human life and property so long as the search is conducted in good faith and with reasonable scope and the passengers have advance notice).

40. Samson v. California, 547 U.S. 843, 843 (2006).

a reduced expectation of privacy in their identity.[41] By this reasoning, anyone convicted of a felony and either in prison or on conditional release (the federal equivalent of parole) is "not entitled to the full panoply of rights and protections possessed by the general public. Quite to the contrary . . . those who have suffered a lawful conviction are properly subject to a broad range of restrictions that might infringe constitutional rights in free society . . . ."[42]

Additionally, probable cause is not needed in searches to obtain information for which the government has a special need beyond the normal need for law enforcement, and adherence to the warrant-and-probable-cause requirement would be impracticable. For example, a special non-law enforcement need is to protect public safety, which has been used to justify drug testing railway workers in order to prevent train accidents.[43] This is called the special needs test. This special needs exception has also been used to justify collecting DNA from convicted felons[44] and may justify collecting blood spots from newborns.[45]

Policies of taking DNA from arrested people who have not been convicted face ongoing challenges. Twenty-one states and the federal government allow law enforcement to collect DNA from a person after he has been arrested for certain offenses, and this practice is likely to spread.[46] New York is considering a new law that would require collecting DNA samples from anyone convicted of any crime, including low-level misdemeanors.[47] And in May 2010, the U.S. House of

41. The Ninth, Fourth, and Fifth Circuits, a Seventh Circuit Judge, numerous federal district courts, and a variety of state courts have applied the totality of the circumstances test to uphold DNA testing of convicted felons. *See, e.g.*, United States v. Kincade, 379 F.3d 813, 832 (9th Cir. 2004); Green v. Berge, 354 F.3d 675, 680–81 (7th Cir. 2004) (Easterbrook, J., concurring); Groceman v. U.S. Dep't of Justice, 354 F.3d 411, 413–14 (5th Cir. 2004); Velasquez v. Woods, 329 F.3d 420, 421 (5th Cir. 2003); Jones v. Murray, 962 F.2d 302, 306–07 (4th Cir. 1992).

42. *Kincade*, 379 F.3d at 833 (internal quotations omitted).

43. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 639 (1989) (allowing drug and alcohol tests for railway employees to prevent accidents). *See also* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 685 (1989) (allowing drug tests for United States Customs Service employees who apply to be in a position overseeing possible drug trafficking).

44. The Second, Seventh, and Tenth Circuits, as well as some state supreme courts, have applied the special needs doctrine to uphold DNA testing of convicted felons. *See, e.g.*, *Green*, 354 F.3d at 679; United States v. Kimler, 335 F.3d 1132, 1146 (10th Cir. 2003); Roe v. Marcotte, 193 F.3d 72, 79–82 (2d Cir. 1999); State v. Martinez, 78 P.3d 769, 771–75 (Kan. 2003); State v. Olivas, 856 P.2d 1076, 1085–86 (Wash. 1993).

45. Most states allow parents to opt-out of the mandatory genetic testing, and courts have not yet had occasion to review the constitutionality of the blood spot collection and testing. It has been posed that the special needs exception would justify the collection if challenged. David H. Kaye et al., *Is a DNA Identification Database in Your Future?*, CRIM. JUST., Fall 2001, at 4, 10.

46. Nat'l Conference of State Legislatures, *supra* note 25.

47. Michael Virtanen, *N.Y. Governor Pushes to Include Misdemeanor Offenders in DNA*

Representatives voted 357–32 to approve legislation to provide funding to states that require DNA samples to be collected from arrestees.

Several cases challenge whether it is reasonable to collect DNA from persons who are arrested[48] or released on bail,[49] but who have not been convicted. In these cases, most courts have applied the totality of the circumstances standard and found that an arrestee has no privacy interest in their identity.[50] Some courts, however, have held that collecting DNA from people who are arrested without a warrant violates the Fourth Amendment, in part, because the collection of DNA implicates more than identity.[51]

Although courts have examined the legality of different types of searches and seizures involved in collecting DNA, courts have not discussed how the Fourth Amendment controls the manner in which DNA can be analyzed after it is seized and initially analyzed. When the legality of mandatory DNA collection is challenged, the courts are "limited to resolving the constitutionality of the program before [them], as it is designed and as it has been implemented."[52] In reviewing the programs immediately before them, courts in every circuit have upheld analyzing DNA taken from convicted felons for the thirteen CODIS loci, which is the standard practice in forensic DNA labs across the U.S.

Database, LAW.COM, June 23, 2010, http://www.law.com/jsp/article.jsp?id=1202462914709&rss=newswire.

48. Anderson v. Commonwealth, 634 S.E.2d 372 (Va. Ct. App. 2006) (upholding DNA collection from arrestees), *aff'd*, 650 S.E.2d 702 (Va. 2007); *In re* Welfare of C.T.L, 722 N.W.2d 484 (Minn. 2006) (finding that portions of a Minnesota statute that direct law-enforcement personnel to take a biological specimen from a person who has been charged but not convicted violate the Fourth Amendment); United States v. Mitchell, No. 09-4718, 2011 WL 3086952 (3d Cir. July 25, 2011) (holding that the federal DNA Act, by allowing the collection and testing of an arrestee's DNA, did not violate the Fourth Amendment); United States v. Purdy, No. 8:05CR204, 2005 WL 3465721 (D. Neb. Dec. 19, 2005) (finding DNA collection without a warrant from arrestees unconstitutional); Haskell v. Brown, 677 F. Supp. 2d 1187 (N.D. Cal. 2009) (upholding DNA collection from arrestees).

49. United States v. Pool, 621 F.3d 1213, 1223 (9th Cir. 2010) (upholding DNA collection as a condition of pretrial release), *reh'g en banc granted*, No. 09-10303, 2011 WL 2151202 (9th Cir. June 2, 2011).

50. *Mitchell*, 2011 WL 3086952 (upholding DNA collection from arrestees); *Haskell*, 677 F. Supp. 2d at 1187 (upholding DNA collection from arrestees); *Anderson*, 634 S.E.2d at 375 (upholding DNA collection from arrestees); *Pool*, 621 F.3d at 1223 (upholding DNA collection as a condition of pretrial release).

51. *Purdy*, 2005 WL 3465721 (finding DNA collection without a warrant from arrestees unconstitutional); People v. Buza, No. A125542, 2011 WL 3338855, at *12 (Cal. Ct. App. Aug. 4, 2011).

52. United States v. Kincade, 379 F.3d 813, 883 (9th Cir. 2004).

C. Additional Tests Already Conducted, but Not Yet Judicially Evaluated

Although testing for the thirteen CODIS markers is the only testing technique that has been explicitly vetted by the courts, in many states DNA analysis already extends beyond this standard practice. Some states are also testing stored DNA for information about familial relationship or using it in medical and academic research. No court has yet evaluated the constitutionality of these additional tests to determine whether they are reasonable searches or whether they constitute searches at all.

As mentioned above, in at least twelve states, law enforcement has begun pulling stored tissue samples to conduct genetic testing at additional DNA loci selected because they contain information about a person's family tree.[53] When comparing the DNA profiles from a crime-scene sample to the profiles uploaded in a database, police analysts may use a less stringent threshold for identifying matches.[54] Lower stringency tests may identify profiles that match some but not all of the crime scene profile, which is likely when two people are related.[55] After police find a partial match in the database, they are permitted to conduct additional genetic tests—usually Y-STR typing—on retained tissue samples to confirm a familial tie.[56]

When analysts make assumptions about familial relationships based only on the thirteen CODIS loci, there are a large number of false positives.[57] Conducting the additional Y-STR typing makes familial matching policy more accurate.[58] Although Y-STR typing increases the accuracy of familial matching and does not require any additional DNA collection, the practice may not spread quickly because of the "potential legal obstacles to retyping samples to generate Y-STR profiles."[59]

---

53. Y-STR typing is discussed *supra* p. 1294–95. *See also* Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248 (2006).

54. Lower stringency comparisons allow police to identify matches even when the crime scene sample is a mix of multiple persons' DNA or when it is incomplete.

55. These partial matches that identify possible family members of would-be suspects occur inadvertently when a police officer intends to find an exact match and requires no information beyond what has already been searched and uploaded into the database. New York is the most recent state to allow lab analysts to report these partial matches to law enforcement so the police can investigate those leads. Press Release, John Caher, N.Y. State Div. of Criminal Justice Servs., Forensic Science Commission Approves "Partial-Match" DNA (June 4, 2009), *available at* http://www.criminaljustice.state.ny.us/pio/press_releases/2009-06-04_pressrelease.html.

56. *See* Ram, *supra* note 17, at 754, 782; *see, e.g.*, Press Release, Anderson, *supra* note 14 (describing policy for Y-STR typing in California).

57. *See* Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 292 (2010).

58. *Id.* at 315.

59. *Id.* at 343.

No court has decided whether Y-STR typing is a Fourth Amendment search or, if it is, whether it is a reasonable search. One could argue that Y-STR typing is just a refinement of the initial search for identification, using twenty-three STR loci instead of the common thirteen STR loci. On the other hand, Y-STR typing is effective precisely because it reveals more than identity; it reveals whether two men likely share a male relative. And in conjunction with the level of similarity between those two men's thirteen CODIS markers, analysts can infer how closely those two men are related.

Stored DNA samples are also being accessed and tested for medical research. In Alabama, the same statute that requires DNA be taken from convicted felons also explicitly authorizes the analysis of that DNA to aid in medical research.[60] Michigan also authorizes the use of its law enforcement DNA database for academic and research purposes.[61]

In addition to DNA taken through the criminal justice system, DNA taken from newborns has also been used for medical research without the parents' knowledge or consent. As mentioned previously, all states require that newborns be screened for genetic diseases by collecting a small amount of blood on a paper card.[62] In Texas and Minnesota, without notifying the parents that the blood spots would be stored indefinitely, these blood spots have been stripped of identifying information to the extent possible and lent to medical and forensic research projects.[63]

Parents in both Texas and Minnesota brought lawsuits in federal court against the states alleging that the additional testing done on their newborn's DNA violated their children's Fourth Amendment rights, but neither of these lawsuits provided clear answers on whether the additional testing is a Fourth Amendment search. In Minnesota, the plaintiffs' Fourth Amendment claim did not survive the motion to dismiss because the district court found they had failed to state a claim upon which relief could be granted.[64] In contrast, the Texas plaintiffs' Fourth Amendment claim survived a motion to dismiss; the district court judge found that the plaintiffs had pleaded enough facts to state a

60. ALA. CODE 1975 § 36-18-20(j) (2010).

61. MICH. COMP. LAWS ANN. § 28.176(d) (2010).

62. Hiraki & Green, *supra* note 29.

63. Letter from Eldridge T. Hutcheson, Laboratory Operations Unit, Tex. Dept. of State Health Servs. to Thomas Parsons, Chief Scientist, Armed Forces DNA Identification Lab. (Mar. 7, 2005), *available at* http://static.texastribune.org/media/documents/DSHS_Letter_To_Feds.pdf.

64. Bearder v. State, No. 27-CV-09-5615, slip op. at 11 (Minn. D. Ct. Nov. 24, 2009), *aff'd*, 788 N.W.2d 144 (Minn. Ct. App. 2010), *cert. granted*, No. A10-101, 2010 Minn. LEXIS 709 (Minn. Nov. 16, 2010).

plausible claim under the Fourth Amendment.[65] Ultimately, the case settled and the state government agreed to destroy more than five million remaining blood spot cards.[66] Neither of these cases was fully adjudicated, and the cases provide no guidance about whether the additional medical analysis of the DNA samples was a new Fourth Amendment search.

These practices demonstrate that although DNA is collected initially for a particular purpose, as long as the government retains it, the sample might be subject to additional analyses, revealing other personal information. Apart from constitutional protections, some additional analyses of the DNA are prohibited by statute and internal law enforcement rules, which differ from state to state.[67] These statutes and rules, however, may change over time to allow other constitutionally permissible DNA testing.

II. THE PROBLEM WITH LIMITING DNA SEARCHES ONLY AT THE TIME OF COLLECTION

As the law currently stands, it is unclear whether there are any limits to what the government may do with DNA once it is legally collected and partially analyzed. State governments are already analyzing stored DNA samples for new purposes. It is possible that some courts might not see any role for the Fourth Amendment in regulating these new analyses of DNA that has already been collected. These courts might follow the reasoning of Justice Scalia in his dissent in *Ferguson v. City of Charleston* that the taking and drug testing of urine presented "only one act that could conceivably be regarded as a search . . . : the *taking* of the urine sample."[68]

If the Fourth Amendment has no role in protecting DNA after it has been collected, then the worries voiced by plaintiffs and amici in *United States v. Kincade*, and by many opponents of warrantless DNA collection, may be realized. "It is inevitable that as technology advances, at some point, [DNA samples] will be used for other purposes

65. Beleno v. Lakey, No. 5:09-CV-00188-FB, slip op. at 15 (W.D. Tex. Sept. 17, 2009), *dismissed per stipulation* (W.D. Tex. Dec. 14, 2009).

66. Jay Root, *Texas Officials Agree to Destroy Babies' Blood Samples After Settling Lawsuit*, DALLAS MORNING NEWS, Feb. 14, 2010, *available at* http://www.texascivilrightsproject.org/?p=1822.

67. *Compare* ALA. CODE 1975 § 13-18-31 (2010) (allowing for medical research uses), *with* CAL. PENAL CODE § 295.1(a) (West 2010) (limiting DNA analysis to identification), *and* S.C. CODE ANN. § 23-3-610 (2010) (permitting law enforcement, non-law enforcement, and humanitarian purposes). *See also* Press Release, Anderson, *supra* note 14 (codifying Y-STR typing protocol for familial searching).

68. Ferguson v. City of Charleston, 532 U.S. 67, 92 (2001) (Scalia, J., dissenting).

without the consent or knowledge of the individual tested."[69] And "soon, if not already, scientists will request access to what would serve as [a] preexisting goldmine of DNA data for their research."[70]

In *Kincade*, although the majority acknowledged these concerns were "weighty ones" and did "not dismiss them lightly," they specifically declined to address how the Fourth Amendment would apply if those analyses became reality; that issue remains unresolved.[71] In order to prevent these future analyses, Judge Reinhardt argued that DNA collection should not be permitted because "[i]t is better to keep the wolf out of the fold, than to trust to drawing his teeth and talons after he shall have entered."[72] Now that the constitutionality of DNA collection has been upheld in many circumstances and the proverbial wolf has been let in, is he permitted to bite?

If the only act that could be regarded as a search were the taking of DNA from a person's body and its initial analysis, a large amount of genetic information would be unprotected. Although limiting the initial government intrusion and collection of evidence is sufficient to protect a person's expectation of privacy in many searches, DNA is distinct from other types of seized materials in ways that make applying Fourth Amendment law more complicated. Specifically, genetic information is intermingled, and the government will be unable to avoid seizing irrelevant, private information with sought-after evidence. As a result, particularity will not be able to precisely limit what information can be seized. Additionally, the intermingled genetic information will be stored, sometimes indefinitely, after its initial analysis, making it available for future testing and amplifying the risk of any gaps in Fourth Amendment protection.

A. Intermingled Information and Particularity

Typically when police conduct a search, they are permitted only to seize particular material. If a search is conducted pursuant to a warrant, then the warrant must state the particular location to be searched and the particular items to be seized; this specificity is called the particularity requirement.[73] When a search is conducted pursuant to an exception to

69. United States v. Kincade, 379 F.3d 813, 837 n.33 (9th Cir. 2004) (citing Brief of Amicus Curiae Protection & Advocacy, Inc.).

70. *Id.* (citing Brief of Amicus Curiae Electronic Information Privacy Center).

71. *Id.* at 837.

72. *Id.* at 844 (Reinhardt, J., dissenting) (quoting THOMAS JEFFERSON, NOTES ON THE STATE OF VIRGINIA 121 (William Peden ed., 1955)).

73. Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents

the warrant requirement, there is no formal particularity requirement, but the circumstances of the exception similarly limit what police may seize.

By allowing the police to search for and seize only particular evidence, the Fourth Amendment limits the extent of the police intrusion into the individual's privacy. For example, when police enter a home to seize a particular piece of evidence, such as a gun, the police may only search for that gun.[74] It is a one-step process that is limited with respect to time, and it ends when the gun is located and seized. Although some additional testing of the gun could be performed, the analysis of the gun could not reveal much information beyond the information immediately relevant to an investigation.

Searching DNA, however, always requires a two-step process: first, searching for and seizing the specimen, and second, extracting the information contained in the specimen. The genetic information in DNA must be analyzed in a laboratory to yield the sought-after evidence and could also reveal a large amount of information unrelated to the crime. Because the DNA specimen contains a large amount of data and testing cannot occur at the time of the initial seizure, the police will need to seize the specimen. Consequently, despite the particularity requirement, the police must seize information in which they have no interest because that information is intermingled with the criminally relevant information in the specimen.[75]

B. Retained Indefinitely and Future Technology

Usually, the specimen containing the DNA will be stored, sometimes indefinitely, after its initial analysis, making it available for future testing and amplifying the risk of any gaps in Fourth Amendment protection. Typically, when police have lawfully seized material but that material no longer serves any state interest (often because the investigation or trial has ended or the property was not useful evidence), an individual can move under Rule 41(g) of the Federal Rule of Criminal Procedure to have the property returned.[76] Rule 41(g) allows "[a] person aggrieved by an unlawful search and seizure of property or

the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

74. If, however, during a reasonable search, police inadvertently discover anything that is immediately apparent to be evidence or contraband, they may seize that additional evidence or contraband under the plain view exception. Arizona v. Hicks, 480 U.S. 321, 326 (1987) (applying "plain view" doctrine to evaluate police officer's moving stereo equipment to read its serial numbers).

75. Of course, the problem of intermingled information is not limited to DNA. As discussed *infra* at p. 1312, courts have addressed this issue with respect to intermingled papers and computer files.

76. FED. R. CRIM. P. 41(g) advisory committee's notes on 1989 amendments.

by the deprivation of property may move for the property's return."[77] The rule requires federal law enforcement to return property that is no longer needed by law enforcement to its owner (unless it is contraband or an instrumentality of a crime), even when that property was seized legally.

Requiring a DNA sample to be returned after it has been analyzed for its evidentiary purpose is not as simple. In May 2010, the Ninth Circuit remanded a case, *United States v. Kriesel*, to a district court in the Western District of Washington to determine whether a former supervised releasee can move under Rule 41(g) to have his DNA sample returned.[78] In this case, Kriesel had provided six drops of blood to a United States Probation Officer, which were sent to the FBI. The FBI used three of these drops of blood to create Kriesel's CODIS profile and stored them in a controlled access storage area. The FBI stored the other three drops of blood in a controlled-access freezer.[79] Kriesel moved under Rule 41(g) to get his blood back.[80]

On July 21, 2011, the district court denied Kriesel's motion and held that

> Kriesel's blood sample is property within the meaning of Rule 41. The Government needed to show it had a legitimate reason for retaining the blood sample to defeat Kriesel's Rule 41(g) Motion. Maintaining CODIS' integrity is a legitimate reason for the Government to retain Kriesel's blood sample. The Government needs to retain [the three drops of blood that had been analyzed] for quality assurance and needs to retain [the three drops of blood that had not been analyzed] as backup to CODIS.
>
> This Court refuses to order the return of the blood sample because the blood was collected for a lawful statutory purpose, Kriesel's claimed harm is speculative, and Rule 41(g) was not meant to resolve policy disputes such as this one.[81]

As Kriesel demonstrates, a motion to return a DNA sample under Rule 41(g) may be frustrated for a number of reasons. A person is not harmed by the deprivation of the use of their seized DNA sample in the same way one is harmed by the deprivation of property like an overcoat. Thus, the moving individual's claim will likely always be "an extremely speculative claim for the return of property with no economic value, and the return of this property would upset a law enforcement system

77. FED. R. CRIM. P. 41(g) (emphasis added).
78. United States v. Kriesel, 604 F.3d 1124 (9th Cir. 2010).
79. United States v. Kriesel, No. 03-05258, slip op. at 3–4 (W.D. Wash. July 21, 2011).
80. *Id.* at 2.
81. *Id.* at 13–14.

authorized by Congress."[82] Courts therefore will be unlikely to order the return of a lawfully collected DNA sample if doing so would "disrupt CODIS with an inconspicuous rule of criminal procedure."[83]

In addition to allowing the collection of DNA, many DNA statutes expressly indicate that the government has a continuing interest in retaining DNA samples. Currently, the federal government and many states retain DNA samples collected for law enforcement or another purpose—not just the personal identification profiles, but the actual specimens.[84] Approximately twenty-eight states have DNA database statutes that do not mention whether the samples should be stored or destroyed.[85] At least six states require samples be retained between thirty-five years and indefinitely[86] and have some restrictions on how the unused samples can be tested.[87] Approximately, thirteen states set up procedures whereby samples may be retained but do not explicitly require it.[88] By contrast, Wisconsin requires all samples be destroyed after DNA analysis is performed.[89] The justification for retaining these samples is to ensure that samples can be reexamined for quality assurance and for retesting when new technologies improve DNA identification analyses.[90]

Storing the samples, however, increases the possibility that they will be tested to reveal more information about a person than was

82. *Id.* at 13.

83. *Id.*

84. The European Court of Human Rights held that storing the DNA of unconvicted people violates European privacy guarantees. S. v. United Kingdom, App. Nos. 30562/04 & 30566/04, ¶ 134 (Eur. Ct. H.R. Dec. 4, 2008). Many legal scholars, even those in favor of expansion of DNA collection, have suggested that the United States' genetic privacy issues would be greatly reduced by similarly destroying the DNA samples after they are tested. *See, e.g.*, D. H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413, 438.

85. This number is based on a survey of state statutes performed in 2004 and, thus, is only approximate. SETH AXELRAD, AM. SOC'Y OF LAW, MED. & ETHICS, SURVEY OF STATE DNA DATABASE STATUTES (2004), *available at* http://www.aslme.org/dna_04/grid/guide.pdf.

86. *See* NEB. REV. STAT. § 29-4105(4) (2010); ARIZ. REV. STAT. ANN. § 13-610(H)(3) (West 2011); CONN. GEN. STAT. ANN. § 54-102i (a) (2011); GA. CODE ANN. § 24-4-62 (West 2010); VA. CODE ANN. § 19.2-310.4 (2010); S.D. CODIFIED LAWS § 23-5A-18 (West 2011); *see also* AXELRAD, *supra* note 85.

87. *See* NEB. REV. STAT. § 29-4105(3) (2010); ARIZ. REV. STAT. ANN. § 13-610(I) (West 2011); CONN. GEN. STAT. ANN. § 54-102i (a) (2011); GA. CODE ANN. § 24-4-62 (West 2010); VA. CODE ANN. § 19.2-310.4 (2010); S.D. CODIFIED LAWS § 23-5A-18 (West 2011).

88. *See supra* note 85.

89. WIS. STAT. ANN. § 165.77(2)(a)2 (2010).

90. 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 24 (2000), *available at* http://www.ncjrs.gov/pdffiles1/nij/183697.pdf.

contemplated when the sample was originally seized.[91] DNA that is reasonably collected today, given what testing can currently reveal and how it is now being used, will still be in the custody of law enforcement when advances in technology make DNA more informative. Storing the samples also increases the risk that they could be analyzed for illegitimate purposes currently prohibited by state laws, such as testing for disease risk or selling the information to insurance providers.[92] Although the laws vary from state to state, most states allow only persons whose convictions have been overturned or who were never convicted to petition to have their samples destroyed and profile expunged, leaving anyone who is convicted without opportunity to have her sample destroyed.[93] Any risk to privacy presented by gaps in Fourth Amendment protection for DNA analysis is made more serious because, in contrast to other types of seized materials that no longer serve an evidentiary purpose, the government can store DNA indefinitely.

C. Large Volume of Private Information in a Small Space

Because each DNA sample contains a large volume of information and the sample can be retained by the government, it is important to determine what protectable privacy interests remain after the sample has been initially tested. Once material has been searched, privacy interests in the material are extinguished. For example, if police are permitted to open and search a closed container, they may look at anything inside that container.[94] Its contents are exposed, and searching those contents more thoroughly does not expand the scope of the search.[95] The zone of the search extends to anything within the container's walls. If

91. *See* discussion of Y-STR typing *supra* p. 1294–95.

92. One article has suggested that these ex-felons could instead "convince the courts to grant them injunctive relief in the form of a bar on any further DNA analysis given the lack of reasonableness of the search." Jason Tarricone, *"An Ordinary Citizen Just Like Everyone Else": The Indefinite Retention of Former Offenders' DNA*, 2 STAN. J. C.R. & C.L. 209, 245 (2005).

93. Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role For Privacy?*, 34 J.L. MED. & ETHICS 153, 158 (2006).

94. United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990) (finding that federal agents' search of box and videotapes found therein, where the box had been opened by employees of private shipper, did not exceed the scope of prior private searches for Fourth Amendment purposes simply because the federal agents took more time and were more thorough than the shipper's agents). *See also* United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001). *Contra* United States v. Rouse, 148 F.3d 1040, 1041 (8th Cir. 1998) (finding that, while law enforcement agents could seize multiple identification cards already discovered during a private search by airline officials, seizing a laminating machine and materials in the same bag that were not discovered by the airline officials or in plain sight violated the Fourth Amendment, because the defendant's expectations of privacy had not already been extinguished).

95. *Simpson*, 904 F.2d at 610.

something is contained in a different, closed container, then it remains private, and opening the container intrudes upon new privacy interests. Constitutional protections will apply to prohibit additional analyses of specimens only if a reasonable expectation of privacy remains in material that has been partially, lawfully analyzed.

As already described, DNA contains a large amount of information about identity, genealogy, and phenotypic traits. All this information is contained in each nucleus of every one of our bodies' cells. As technology advances, more meaningful information will be extractable from that genetic material. While the size of the space being searched predictably limits the amount of information stored in a room within a house or a container, the only practical limit on information that can be extracted from biological samples are currently-available analysis techniques and our knowledge of what genetic variations mean.

Additionally, a person typically knows what she has brought into her house and stored there, but a person has no reason to know much of the information that will be revealed when her DNA is analyzed.[96] A person has little to no discretion over what information is stored in her body and likely has not analyzed or evaluated that information herself. A person's privacy in the contents of each microscopic bundle of DNA should be more stringently protected because of the unpredictability and density of the genetic information it contains.

It must be determined whether, and in what, a reasonable expectation of privacy remains after any laboratory analysis of specimens collected for DNA information has been conducted. To what extent does permitting a search for some information extinguish the privacy in all the information contained in a biological sample?

III. DIGITAL COMPARISON AND HOW TO LIMIT DNA ANALYSIS

Differences exist between applying Fourth Amendment protection to laboratory analysis and to more traditionally protected contexts. But under the logic of the Fourth Amendment, an individual's privacy interest in her genetic information should be constitutionally protected.

Recently, in evaluating whether collecting DNA from an arrestee violated the Fourth Amendment, the Third Circuit reasoned that "[t]he collection of DNA . . . entails two separate 'searches.' The first is the physical collection of the DNA sample."[97] "The second 'search' at issue is, of course, the processing of the DNA sample and creation of the

96. Some of the genetic information would be known. For example, one would expect DNA to show one's sex and some inherited traits.

97. United States v. Mitchell, No. 09-4718, 2011 WL 3086952, at *17 (3d Cir. July 25, 2011).

DNA profile for CODIS. This search also has the potential to infringe upon privacy interests."[98] Thus, the court made clear that the initial DNA testing is a search within the meaning of the Fourth Amendment.[99]

But the question remains whether a second or third analysis of that same specimen would require Fourth Amendment scrutiny. To answer this question, we must consider "the relatively undeveloped and critical issue of whether, sometimes, the mining of information from materials already in the government's possession might constitute the invasion of a reasonable expectation of privacy."[100]

Given the characteristics of DNA discussed above, principles that define the scope of a search by limiting the initial intrusion at the time of collection are insufficient to limit the scope of DNA analyses, which allow a large amount of personal information to be tested long after the DNA is collected. In order to apply Fourth Amendment principles in a way that better suits DNA analysis, we should examine how courts have applied constitutional limits to other technologically-advanced searches that present similar complications and extend that reasoning to DNA. Thus, this Article looks to a non-biological area of technology law in which the issue of how to define the zone of a search in an information-rich context that may be subject to subsequent analyses has been more thoroughly explored: government searches of computers.

Computers and DNA share characteristics that distinguish both from more traditionally protected zones of privacy. They both store a large amount of intermingled information in a small space that cannot be parsed at the time of collection. Cases challenging novel and broad searches of computers have given courts the opportunity to thoroughly analyze how the Fourth Amendment applies in this type of technologically advanced context.

Computer-search law is not wholly different from the law addressing more traditional searches. Rather, the benefit of computer-search law is that it develops analogies by which to extend traditional Fourth Amendment principles to a challenging new context. These computer cases are the best indicators of how courts may apply constitutional rules to the different ways in which DNA can be analyzed. Computer-search law is not uniform across jurisdictions. Different courts have applied the

98. *Id*. at *18.

99. Similarly, several cases that evaluated mandatory drug-testing have held that chemical laboratory analysis of urine specimens is an invasion of privacy warranting Fourth Amendment scrutiny. *See* Chandler v. Miller, 520 U.S. 305, 313 (1997); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 617 (1989); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989).

100. Sherry F. Colb, *Does Routinely Sampling DNA from Arrested Felons Violate the Fourth Amendment?*, FINDLAW, Nov. 10, 2010, http://writ.news.findlaw.com/colb/20101110.html.

Fourth Amendment in different ways to limit searches of computers. Comparing different approaches to regulating computer searches provides interesting parallels to regulating DNA analysis; these parallels are predictive of how courts are likely to evaluate the reasonableness of new DNA analyses and create the basis for this Article's recommendations on which rules courts should apply.

By examining the emerging law on computer searches, it is possible to identify effective and doctrinally-supported approaches to striking the appropriate Fourth Amendment balance between protecting individuals' genetic privacy and ensuring that the government can collect valuable DNA evidence and information. The optimal rules are ones that interpret the Fourth Amendment to require a warrant or warrant exception before running additional tests on the DNA.

A. Zone of Computer Searches: Physical-Device or Virtual-File

First, this Article looks at how courts have defined the zone of a computer search and what that indicates for defining the zone of a DNA search. As mentioned above, once material has been searched, privacy interests in the material are extinguished. The material can be searched again more thoroughly, without any justification required. Looking at something that falls within the zone of the initial search is not a new Fourth Amendment action. If something is outside the zone of the initial search, however, it remains vested with its original expectation of privacy, and searching that material must be justified and reasonable.

In many searches, determining the zone of what has already been searched is simple: when police open a container, everything in that container is within the zone of the search. Traditionally, Fourth Amendment law has focused on whether it is reasonable to penetrate the boundaries of a physical space. Once those boundaries are penetrated, privacy in that zone is extinguished. Determining what expectations of privacy have already been compromised by an initial search is more difficult when there are no physical walls to define the zone of that search. To extend this principle to laboratory searches, one must define what privacy interests are compromised when a search is conducted in a much smaller space, like the inside of a hard drive or a human cell. This inquiry is critical to determining what information remains private after police have analyzed some information in a computer or for that matter a DNA sample.

As Orin Kerr explains in *Searches and Seizures in a Digital World*, courts have used two different bases for defining the zone of a search and determining what remains private after a computer search begins:

(1) the boundaries of the physical device, and (2) the effort necessary to open another file.[101]

The "physical device approach"[102] to defining what privacy interests remain after a search has been adopted in some cases that involve searches of digital information stored on a computer. Some digital search cases have held that physical parts of a computer device constitute containers that hold information, which ceases to be private once the container is opened.[103] For example, in *United States v. Runyan*,[104] the Fifth Circuit compared a disk containing multiple files to a single container and found that no privacy interest remained in a disk once some of its contents had been viewed: thus, all other files on that disk could be opened. Regarding the unopened disks, the court found privacy rights to be intact and held unlawful a warrantless search of such disks.

In *United States v. Crist*,[105] a federal district court adopted this approach when determining whether a hard drive is analogous to a single closed container. In *Crist*, the court concluded that a hard drive is not a single closed container, but the individual platters or magnetic data storage units that are mounted together to compose a hard drive are analogous to the disks in *Runyan*.[106] Both of these cases involved an initial search conducted by a private person and a second search conducted by the police. The *Runyan* and *Crist* courts reasoned that the physical boundaries of the device defined what information remained private after the initial private search and what could be searched more thoroughly during the second search.

Other digital search cases have moved away from this more traditional focus on whether physical walls have been penetrated and instead focus on the content of what has been revealed. These cases peg the contours of the search to a "virtual file approach."[107] These cases treat individual files as separate containers, whereby the opening of each file must be justified.[108] In *United States v. Carey*,[109] the Tenth Circuit

101. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554–56 (2005) (describing the "physical device approach" and the "virtual file approach").

102. *Id.* at 554.

103. United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (finding that the initial private search extinguished a reasonable expectation of privacy in the disk that was searched but not in other disks that were also turned over to police by the private party).

104. *Id.*

105. United States v. Crist, 627 F. Supp. 2d 575 (M.D. Pa. 2008).

106. *Id.* at 586.

107. Kerr, *supra* note 101, at 555 (discussing the "virtual file approach").

108. *See, e.g.*, United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

109. *Id.*

held that a warrant granting access to the defendant's computer to search for files containing evidence of drug trafficking did not allow police to open other files to instead look for evidence of child pornography. Opening additional files expanded the search and violated distinct privacy rights.

Even more restrictive, Judge Bea's concurring opinion in *United States v. Comprehensive Drug Testing*, a recent Ninth Circuit case, considers only the information made visible on the screen as being searched, requiring there to be a separate justification for moving the scroll bar to the right and thereby exposing more information.[110] Judge Bea distinguishes the zone of what has been searched not by the file, but by what data is exposed on the screen. This reasoning aligns with Orin Kerr's argument that the zone of a computer search "should be whatever information appears on the output device" explaining that this comports with the virtual file approach because "an analyst who takes a mouse, clicks, pulls down the file to see other parts of the file not previously exposed has done nothing different from another analyst who double clicks on a second file to open it. . . . Both actions should be treated as searches."[111]

Cases that separate privacy interests by individual files or screen shots do not rely on the physical boundaries of a device. Rather, these cases rely on the content, specifically what information has actually been exposed to the analyst to define the zone of a search. In these cases, opening a new file or moving a scroll bar is similar to opening a new container because they require the investigator to perform an additional step that exposes new information. These cases signal a shift in Fourth Amendment law away from relying solely on the form of the search—what area may be penetrated—toward a focus on the content of the search—what information will be revealed.

Both of these rationales are workable when applied to computers. It takes work to analogize between closed containers and computers, and the physical boundaries approach may seem strained when comparing computer disks or platters to containers. DNA, however, is even one step more removed, and in that context, the physical boundaries approach breaks down altogether.

110. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1017 (9th Cir. 2009) (en banc) (Bea, J., concurring in part and dissenting in part), *revised and superseded by* 621 F.3d 1162 (9th Cir. 2010) (en banc).

111. Kerr, *supra* note 101, at 557.

B. Zone of a DNA Search: Physical Specimen

Borrowing from computer law, there are two ways in which courts may define the zone of a DNA analysis: the "physical specimen" approach or the "exposed information" approach. For both normative and doctrinal reasons, the exposed information approach to defining the zone of a DNA analysis is the far better approach.

1. Description of the Physical Specimen Approach

The physical specimen approach is the parallel to the "physical device" approach used by the Fifth Circuit in *Runyan*, whereby once a hard drive or disk has been accessed, the entire device has been searched and privacy interests in everything else contained on that device are extinguished. The physical specimen approach relies on the same underlying principle as the "physical device" approach that the tangible boundaries of the material define the zone of a search.

The physical specimen approach does nothing to protect a person's genetic privacy after the initial DNA analysis is performed. If one were to define the specimen itself as a single closed container, similar to treating a disk as a single container as the court did in *Runyan*,[112] then everything contained in the sample is no longer private and can be viewed or searched. For example, consider a blood sample collected by police in order to match DNA to a crime scene sample. If one analysis compromises the expectation of privacy of everything in the sample, then the blood sample could also be tested for blood alcohol content, the presence of narcotics, or chromosomal abnormalities linked to disease risk.

There are, of course, smaller physical boundaries within a specimen; this mode of analysis is similar to that of the *Crist* court,[113] which identified the platters instead of the entire hard drive as the appropriate container of digital information, that could be used to construct the metaphorical container walls. But even if the physical boundaries were limited to the membrane around a single nucleus in a single cell, the person's entire library of DNA would be subject to analysis.

Under the physical specimen approach, additional analyses could be performed on any tested and retained DNA sample. Already, some DNA collected for identification and medical screening purposes is used

112. United States v. Runyan, 275 F.3d 449, 458, 461–64 (5th Cir. 2001) (holding the zone of the search was defined by the individual diskettes, and each diskette was equivalent to a closed container).

113. United States v. Crist, 627 F. Supp. 2d 575, 586 (M.D. Pa. 2008) (holding the zone of the search was defined by the individual platters in a hard drive).

for research analyses. Law enforcement is also analyzing DNA, which was originally collected for identification, to show familial relationships. In the future, this familial searching might be done on DNA taken from arrestees, crime victims, former suspects, military personnel, or newborns, all of which might aid in identifying the true perpetrator. Additionally, the government may want to expand the CODIS database by analyzing DNA, originally taken from newborns for medical screening, for identification or familial relationship, in the same way that a convicted person's DNA is analyzed now. Alternatively, in an effort to prosecute statutory rapists or to facilitate the collection of child support, the government might analyze stored DNA for evidence of paternity. In a more far-fetched scenario, if research on behavioral or psychiatric phenotype yields useful information, these stored DNA samples may someday be tested to produce genetic character evidence or to determine a person's legal mental health status for purposes of competency, commitment, sentencing, or benefits eligibility.

2. Related Harms

Without regulation of what tests can be done, individuals whose DNA has been collected will be open to privacy harms. In addition to the dignitary harm done by having personal information exposed, the genetic information yielded from the additional tests or general protocols discussed above—identity, paternity, other familial relationships, ancestry, disease risk, and behavioral propensities—could have negative consequences for the individual. If a person's genetic identification profile is created, that person can be implicated in future crimes and will constantly be compared to crime scene DNA samples, which some have referred to as lifelong "genetic surveillance."[114] Also, if DNA is subject to familial searching, to reveal other family relationships, the individual may feel responsible for making his entire family subject to such genetic surveillance. Furthermore, if a family member were to be subsequently prosecuted for a crime, that individual could feel responsible for implicating their family member.

Information about paternity could be used as evidence of statutory rape if the mother of the child is underage or as evidence in a civil case to require the father to pay child support. Aside from the legal setting, evidence of paternity could also give the child a claim for inheritance or disrupt the father's existing family if he was not previously aware of the child. Additionally, government-conducted paternity testing could harm

114. Jeffrey Rosen, *Genetic Surveillance for All*, SLATE, Mar. 17, 2009, http://www.slate.com/id/2213958.

the mother if it keeps a man involved in her life whom she had hoped to avoid.

Additionally, if a person's DNA is made available for research, a person may be unwillingly supporting research she opposes. For example, some groups of people have declined to participate in genetic ancestry research that might contradict their beliefs about their own ancestry. Recently, members of the Havasupai tribe in Arizona brought a lawsuit against Arizona State University for genetic research conducted without their consent, which indicated that the tribe had Asian ancestry in contradiction to the tribe's traditional stories about its origin.[115] A person whose DNA is taken and later used in research will have no say over the type of research conducted, the results of which may affect how she understands herself.

The phenotypic information revealed by genetic testing could also harm a person if disclosed, although some of these harms are speculative and contingent on advances in medical, behavioral, and psychiatric research that have not yet been realized. Genetic testing for disease risk, if shared with insurers, could result in a person being denied life insurance, disability insurance, or long-term care insurance.[116] If disclosed to the person, who would not have wanted to know, it could change the person's plans in an undesired way.[117] If a person is revealed to have a gene associated with a psychiatric disorder, it might support a finding that the person should be institutionalized or is incompetent. On the other hand, if a person claiming to have a psychiatric disorder for mitigating a criminal sentence or to receive government benefits is found not to have a strongly associated gene, that information might be used to counter the person's claims. Lastly, and most speculatively, information about whether a person has a gene variant associated with behavior, for example violent behavior, might be used to direct an investigation or to predict recidivism for sentencing[118] and parole decisions.

Basing Fourth Amendment protection on the spatial boundaries of a DNA specimen would allow unchecked DNA analysis and would have

115. Amy Harmon, *Indian Tribe Wins Fight to Limit Research of its DNA*, N.Y. TIMES, Apr. 22, 2010, at A1.

116. None of these are affected by the Genetic Information Nondiscrimination Act ("GINA"). Mark A. Rothstein, *Putting the Genetic Information Nondiscrimination Act in Context*, 10 GENETICS IN MEDICINE 655, 655 (2008).

117. *See, e.g.*, R. Adorno, *The Right Not To Know: An Autonomy Based Approach*, 30 J. MED. ETHICS 435 (2004) (arguing that people have an interest in not knowing their genetic make up to avoid serious psychological consequences).

118. *See* Emiliano Feresin, *Lighter Sentence for Murderers with 'Bad Genes,'* NATURE NEWS, Oct. 30, 2009, http://www.nature.com/news/2009/091030/full/news.2009.1050.html.

real consequences for the people whose DNA has been collected. Instead, a more content-focused approach would regulate when additional analyses can take place and how those analyses should be conducted.

C. Zone of a DNA Search: Exposed Information

The exposed information approach is similar to the "virtual file" approach used by the Tenth Circuit in *Carey*,[119] whereby only the privacy interests in an opened file have been extinguished. If additional effort would be required to open a new file or expose new information within a file, then that information has not yet been searched and retains its original privacy protections.[120] The additional step necessary to open a new file distinguishes it from what has already been searched, and the same could be true of the additional step necessary to reveal new genetic information; the exposed information approach generalizes this principle to other non-computer contexts.

1. Description of the Exposed Information Approach

Defining the zone of a search based on the exposed information approach is more protective of an individual's privacy. Under this approach, even after some analysis has been done, additional analyses that reveal new information would impinge on the remaining reasonable expectation of privacy in the sample. Analysis that exposes information inside of the physical boundaries of a biological sample or a single cell would not eliminate privacy interests in other information that cell can reveal. Each analysis is an incremental effort that exposes private information, similar to opening a new container, which must be reasonable and justified.

To illustrate the privacy differences between these two approaches, consider a hypothetical posed by three professors in a 2001 article.[121] The article suggested that blood spots taken to test newborns for treatable genetic diseases could also be genotyped at the CODIS markers in order to build a more universal DNA database for criminal law enforcement identification. Taking the newborn blood spots would be justified, as a special needs search, with a primary purpose that has

119. United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that opening a new file exposed information outside the zone of what had already been searched).

120. *See also* Orin Kerr's discussion of the "exposed data" approach to defining the zone of a search. Kerr, *supra* note 101, at 556.

121. Kaye et al., *supra* note 45, at 10.

nothing to do with normal law enforcement. The article argued that identification analysis could piggyback on top of that genetic screening, even though it is useful only for future identification, as a secondary purpose of the same DNA search. This argument conceives of the DNA analysis as a single search with two purposes. Under the physical specimen approach, that analysis would be correct; both of these analyses would be part of the same search. Under the exposed information approach, however, testing for the CODIS markers would be an additional search because it requires steps which expose new information, the steps necessary to genotype those loci.

In addition to protecting privacy, the exposed information approach also allows the government to more easily justify collecting DNA. If a physical specimen approach were adopted, any DNA collection could be challenged because it leaves all of a person's genetic information vulnerable to later searches. The exposed information approach, however, assuages these concerns by requiring that analysis of new information in DNA must be independently reasonable and justified and must pass Fourth Amendment scrutiny.

The exposed information approach is also better supported by case law than the physical specimen approach. In *Ferguson v. City of Charleston*,[122] the Supreme Court held that certain laboratory tests on a biological specimen were unreasonable even though the specimen was previously tested for another purpose. In *Ferguson*, a government-funded hospital had instituted a program in which urine samples collected from certain pregnant patients for medical testing were also tested for the presence of cocaine. If the samples tested positive for narcotics, the hospital reported their findings to the police. The Court held that the additional laboratory testing violated the Fourth Amendment.[123]

The Court recognized that patients retain a privacy interest in information in their urine samples even after consenting to other tests. Their consent prescribed the parameters of what searches could be done. Therefore, if the patients consented only to medical testing related to pregnancy, then that is the extent of what could be searched for.[124] Testing for drug use was an additional step that exposed new information and thus constituted a new search. Unless the patients had

122. Ferguson v. City of Charleston, 532 U.S. 67 (2001) (involving the testing of plaintiffs' urine for evidence of drug use when it was originally taken to test for medical information).

123. *Id.* at 86.

124. The consent serves the same purpose here as the particularity requirement in a search pursuant to a warrant.

consented to the drug testing,[125] it constituted an unconsented to, and in this case, unreasonable search.

The Court's reasoning is better captured by the exposed information approach than the physical specimen approach. The principle that connects *Ferguson* to *Carey* is that any incremental effort that exposes new information is a new Fourth Amendment moment. If one must take an additional step to expose evidence, then that evidence, axiomatically, was not already searched, and the privacy interest in it is retained.[126]

2. Comparative Advantages

Applying the exposed information approach to preserving privacy interests in DNA, it appears that each analysis that provides new results is a search. Although police may have already conducted some tests on a specimen, that analysis does not diminish expectations of privacy in unrevealed information. Furthermore, although that specimen is lawfully in police custody and might be indefinitely retained, the individual's expectation of privacy in its contents is not diminished by that seizure or retention. Additional analyses on biological samples must be reasonable by Fourth Amendment standards, either falling within the scope of the original search or being an independently justifiable search.

Thus, let us apply this standard to Y-STR familial search programs. As detailed above, under this program, if analysts find a partial match between a crime scene DNA sample and a known DNA profile, the stored DNA sample for that known DNA profile will be genotyped at ten additional locations on the Y chromosome to determine whether the crime scene DNA came from that person's close male relative. This Y-STR typing, instead of stopping at the thirteen CODIS loci, is a step that exposes new information and therefore is an additional search triggering a Fourth Amendment analysis. Although on its own, Y-STR genotyping only reveals whether two men share a common patrilineal ancestor, in conjunction with the thirteen autosomal CODIS markers, these Y-STR loci can indicate how closely related the two men are. These additional steps that reveal new information constitute a new search requiring Fourth Amendment scrutiny.

The legal question of how to define the zone of a search determines

125. On remand, the Court of Appeals for the Fourth Circuit found that none of the patients had consented to drug testing. Ferguson v. City of Charleston, 308 F.3d 380, 395, 404 (4th Cir. 2002).

126. *See also* United States v. Lemmons, 282 F.3d 920, 925 n.5 (7th Cir. 2002) (stating, in dicta, that a computer file is not in plain sight when an agent must enter commands into the computer to access the file).

only whether a new search has occurred, not whether that new search is reasonable. Such a search must be reasonable in its own right. Whether the Y-STR typing search is reasonable depends on how strong those privacy interests are and the government's need for the information.

Sometimes these additional analyses will be reasonable without a warrant. For example, although no court has yet reviewed it, Y-STR familial searching programs involving DNA from convicted persons would very likely be found reasonable, especially if Y-STR typing is only performed on specimens that, based on the CODIS loci, were very likely to yield a familial match. If a convicted person's DNA is analyzed, his expectation of privacy in family ties may be part of the "panoply of rights and protections"[127] to which his conviction disentitles him. If so, a warrant would not be required and a totality of the circumstances test would apply.[128] It should be noted that, although Y-STR typing may not require a warrant, that is only one part of the ongoing conversation about whether familial searching is a good policy.[129]

Under that totality of the circumstances test, the government's need for the information is compelling. The government's interest in solving and preventing crime is an important interest; Y-STR typing is performed if the thirteen common STR markers partially match, and Y-STR typing increases the accuracy of familial searching thereby narrowing the number of leads the police must follow.

However, under the exposed information approach, a warrant would likely be needed if Y-STR typing were expanded to other groups of individuals whose DNA has been collected. It has been argued that limiting familial searches to convicts is "legally, logically, and morally unjustified," and it should be broadened to other groups of people—arrestees, voluntary contributors, and crime victims—to offset concerns about the discriminatory impact of familial searching.[130] Under the exposed information approach, this proposal intrudes upon these individuals' privacy interests, which in some cases may require a warrant to be reasonable. For example, performing Y-STR typing on DNA taken from a crime victim who has not lost the same privacy interests as a convicted person would likely require probable cause and a

127. United States v. Kincade, 379 F.3d 813, 833 (9th Cir. 2004) (holding that a conviction lowers a person's expectation of privacy in their identity, and therefore, no warrant or suspicion is required under the Fourth Amendment to collect DNA from a convicted felon and to create an identifying DNA profile).

128. Or, in some jurisdictions, a special needs approach would be used.

129. *See generally* Murphy, *supra* note 57.

130. *Id.* at 41 (generally arguing against familial searching but also exploring best methods if it is used).

warrant.

Defining the zone of a search as only the information that was actually exposed strikes the better balance between privacy interests and the need for evidence collection. It requires the court to consider whether new tests on stored DNA are reasonable. Alternatively, under the physical specimen approach, courts would never reach the reasonableness issue. This approach is also better supported by case law than an approach that bases the zone of a search on the physical contours of the DNA specimen, which would extinguish privacy interests in all the information contained in that specimen.

Additionally, examining these approaches in the novel context of searching a DNA specimen that has already been collected and tested for another purpose illustrates that when a large amount of intermingled information is stored in a small space, it no longer makes sense to base Fourth Amendment protection on penetrating boundaries and the right to enter a space. Instead, as we are able to access more information that is stored in complex ways in systems that are not separated by clear boundaries, Fourth Amendment law will continue shifting to focus more on the content of a search and the information that is revealed.

D. Statutory Alternative

Of course, constitutional protection is not the only way to guard genetic privacy while allowing the government to conduct important analyses. If courts do not limit DNA analysis as a constitutional matter, then legislatures should so limit it. A statute could accomplish the same goals as the Fourth Amendment if it protects individuals from unnecessarily intrusive analyses of their DNA and provides a remedy for the criminal, psychological, and financial harms resulting from violations of the statute or from sharing incidental findings.

States might augment particularity by requiring that applications for a DNA warrant require a particular description of the type of genetic information sought, rather than simply a statement of whose DNA is to be taken and for what general purpose. When DNA is taken and tested without a warrant, the statute itself should limit the purposes for which DNA can be analyzed. Some states already have DNA statutes that do this. For example, California's DNA statute indicates that the state "shall perform DNA analysis and other forensic identification analysis pursuant to this chapter *only* for identification purposes."[131] Other states, however, do not limit the purposes for which DNA can be

131. CAL. PENAL CODE § 295.1 (West 2010) (emphasis added).

analyzed. For example, South Carolina's DNA statute states a very broad purpose, which might include anything: to "develop DNA profiles on samples for law enforcement purposes and for humanitarian and nonlaw enforcement purposes,"[132] which will have several uses, including "generat[ing] investigative leads in criminal investigations."[133] If constitutional limits to analysis do not suffice, it would be important that the legislators reconsider this open-ended approach to DNA analysis and instead impose clear rules regarding the purposes for which DNA can be tested.

These statutes must also include back-loaded privacy protections that limit what happens with genetic information after it is revealed and provide remedies for the individual if the statute is violated. Most state DNA statutes already count unauthorized analysis of stored DNA or sharing the results of DNA analyses as a criminal offense; in most of these states, it is a misdemeanor.[134] These statutory prohibitions penalize the violator with fines and possible jail time.

But most of these statutes are silent about whether the individual whose DNA has been accessed has any remedy. None of the state statutes include any remedy if an unauthorized DNA analysis were to reveal genetic information that could be used as evidence. Even if a DNA analysis violates the statute, a court would not per se exclude any DNA evidence yielded.[135]

Additionally, only a few states mention financial remedies for the individual whose DNA has been accessed in violation of the statute. These states create ceilings or floors for the financial recovery. For example, in California, if a DNA sample is used for any purpose other than criminal identification or if DNA database information is improperly shared, the person whose DNA is affected will receive $5,000 in damages for each violation, up to $50,000, and no other civil liability will attach to the violation.[136] In Nebraska, if a person's DNA sample or genetic information is shared for pecuniary gain, then the person will receive at least $100 in damages.[137] Most states are silent about whether a person can bring a civil lawsuit if their DNA is tested or their genetic information is shared in violation of the statute.

132. S.C. CODE ANN. § 23-3-610 (2010).

133. S.C. CODE ANN. § 23-3-640 (2010).

134. AXELRAD, *supra* note 85 (listing both criminal penalties and civil causes of action given rise to by state DNA laws).

135. People v. Robinson, 224 P.3d 55, 66–67 (Cal. 2010), *cert. denied*, 131 S. Ct. 72 (2010) (holding that DNA evidence would not be excluded because even though its collection was not sanctioned under statute at the time it was collected, the collection was reasonable).

136. CAL. PENAL CODE § 299.5(i)(2)(A) (West 2010).

137. NEB. REV. ST. § 29-4105 (2010).

If these state statutes were to become the only limitations on DNA analysis, then they must also include remedies for the individual who is aggrieved by the unauthorized DNA analysis or data sharing. These remedies should include an exclusionary clause that prevents the new genetic information from being used as evidence in court. Perhaps more importantly, because most of the negative consequences of violating a person's genetic privacy follow from out of court uses, these remedies should also include a cause of action to claim damages arising from the violation.

Additionally, legislatures might consider adopting a notification requirement when new tests are run on a person's DNA. A requirement that individuals be notified when their DNA is tested might guard against unnecessary testing and would give people aggrieved by DNA testing the opportunity to seek remedies.

Currently, this level of statutory protection is unnecessary because the forensic DNA testing methods used now are targeted and focused. If DNA testing methods change to be more varied in scope or more intrusive, then statutes may need to more closely regulate genetic testing.

Although many of the same protections can be accomplished through statute, if the Fourth Amendment is to remain meaningful as technology allows the government to glean more information through laboratory analysis, then the Fourth Amendment principles must account for the realities of these new searches. DNA is just one instance of a technologically advanced search that is hard to limit using Fourth Amendment rules that focus on the spatial boundaries of a search rather than the content of the information revealed by that search.

CONCLUSION

The Fourth Amendment has traditionally focused on whether the boundaries of a particular space can be penetrated, not on what information is contained in that space. The traditional approach still works reasonably well when limiting government intrusion to a computer, but not when applied to a DNA specimen that has already been tested, leaving private genetic information exposed. Some courts applying the Fourth Amendment to regulate searches of computers have developed approaches more sensitive to the information that has been exposed. Drawing from this computer-search case law, this Article proposed that any analysis of stored DNA samples that reveals new information must be both reasonable and justified, requiring either a warrant or an exception to the warrant requirement. Thus, new analyses

like the familial searching that identified a relative of the Grim Sleeper could be conducted. But in situations when the government's need does not justify intruding upon individuals' privacy, the stored DNA will remain undisturbed.

Evaluating the Fourth Amendment in this context indicates that the content of what is exposed by the search, as opposed to the form of the search, will play an increasingly important role in determining what constitutes a search and whether a search is reasonable as investigatory tools are able to capture more information from spaces that lack clear boundaries. For example, other biological specimens also contain a large amount of information in very small spaces, and more of that information is becoming interpretable as science progresses.[138] Under the approach proposed by this Article, privacy interests in these specimens will be protected even after they have been seized, tested, and stored, thus permitting necessary evidence collection without revealing all the secrets hidden in our bodies.

138. For example, microbe communities found in human waste are being studied for forensic uses. S*ee generally* The Nat'l Inst. of Health Common Fund, Human Microbiome Project Program Initiatives, http://nihroadmap.nih.gov/hmp/initiatives.asp (last visited Apr. 4, 2011). And brain-imaging technology allows large volumes of data about brain function to be acquired, which can later be analyzed in different ways, revealing information about how we think and, potentially in the future, revealing what we think. Dov Fox, *Brain Imaging and the Bill of Rights: Memory Detection Technologies and American Criminal Justice*, 8 AM. J. BIOETHICS 34 (2008); *see also* Teneille Brown & Emily Murphy, *Through a Scanner Darkly: Functional Neuroimaging as Evidence of a Criminal Defendant's Past Mental States*, 62 STAN. L. REV. 1119 (2010).