


3-28-2013

No Cilia Left Behind: Analyzing the Privacy Rights in Routinely Shed DNA Found at Crime Scenes

David Gusella

Boston College Law School, david.gusella@bc.edu

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/bclr>

 Part of the [Constitutional Law Commons](#), [Criminal Procedure Commons](#), [Health Law and Policy Commons](#), [Law Enforcement and Corrections Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

David Gusella, *No Cilia Left Behind: Analyzing the Privacy Rights in Routinely Shed DNA Found at Crime Scenes*, 54 B.C.L. Rev. 789 (2013), <http://lawdigitalcommons.bc.edu/bclr/vol54/iss2/9>

This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydowski@bc.edu.

NO CILIA LEFT BEHIND: ANALYZING THE PRIVACY RIGHTS IN ROUTINELY SHED DNA FOUND AT CRIME SCENES

Abstract: As science advances, researchers are learning more about the meaning of information that is contained in the human genome. Because we routinely shed DNA in public, this has significant implications for an individual's ability to keep genetic information private. If routinely shed DNA is found at a crime scene, there is a significant governmental interest to sequence the DNA in order to uncover suspects or potential witnesses. This Note analyzes the implications of advancing technology on an individual's right to privacy in one's own genetic information, and it argues that informational privacy should be protected for non-phenotypic information in routinely shed DNA at crime scenes.

INTRODUCTION

On June 26, 2000, the leaders of the Human Genome Project, along with the private company Celera, announced the completion of the first sequencing of an entire human genome.¹ As scientists sequence more genomes, they are learning that virtually all health conditions are affected to some degree by genetic factors, making genome sequencing increasingly important in predicting susceptibility to certain diseases.² Because a genome contains private medical information, the decoding of a person's genome without consent would seem to violate that individual's privacy.³

People involuntarily and continuously shed genetic material, and any of these stray hairs, skin particles, or other bodily fluids could be

¹ Judit Sandor, *Genetic Information: Science, Society, and Legal Norms*, in SOCIETY AND GENETIC INFORMATION 21, 25 (Judit Sandor ed., 2003); Geoffrey Carr, *Biology 2.0*, ECONOMIST, June 19, 2010, at 3, 3–5. An individual's genome consists of all the genetic information in a person's body. SHELDON KRIMSKY & TANIA SIMONCELLI, GENETIC JUSTICE: DNA DATA BANKS, CRIMINAL INVESTIGATIONS, AND CIVIL LIBERTIES 7 (2011). Although the Human Genome Project was announced as complete in 2000 by Bill Clinton and Tony Blair, the first entirely-sequenced genome was not published until 2003. Carr, *supra*, at 3.

² LORI ANDREWS ET AL., GENETICS: ETHICS, LAW AND POLICY 2 (2002).

³ Amitai Etzioni, *DNA Tests and Databases in Criminal Justice: Individual Rights and the Common Good*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 197, 204 (David Lazer ed., 2004).

used to sequence an individual's entire genome.⁴ Although the utility of information hidden in an individual's genome is limited by current technology, as more genomes are sequenced and understood, the sequencing of entire genomes could be used to help hunt down suspects and solve crimes in the next few years.⁵ Because laws concerning genetic privacy are currently "very sparse and random," genetic privacy regulation is required as technology advances.⁶ This Note focuses on the sequencing of genetic materials left at a crime scene for two reasons.⁷ First, this situation requires balancing the interests of law enforcement in the information that could be provided by sequencing genetic material left at a crime scene against the privacy expectations of individuals in medical information that can be uncovered from such sequencing, which helps define limits on individuals' privacy rights in crime scene DNA.⁸ Second, because any location could become a crime scene, this analysis could apply to any routinely shed genetic material found in a public place.⁹

Part I of this Note discusses the information contained in genetic material.¹⁰ Although scientists can currently only uncover limited information from this genetic material, this Part looks to the future and discusses the potential information that genetic sequencing may be able to provide about an individual.¹¹ Part I also describes how genetic material is currently used in criminal investigations, and the roles genetic sequencing could have in future investigations.¹² Part II analyzes the privacy rights of genetic material by looking at both the existing body of privacy law and the academic arguments regarding privacy in genetic information.¹³ This analysis includes courts' attempts to balance an individual's interest in keeping genetic information private against the investigator's interest in uncovering information without a warrant.¹⁴ From this framework, Part III argues that there should not

⁴ Eriq Gardner, *Gene Swipe: Few DNA Labs Know Whether Chromosomes Are Yours or If You Stole Them*, A.B.A.J. (Aug. 1, 2011, 2:40 AM), http://www.abajournal.com/magazine/article/gene_swipe_few_dna_labs_know_whether_chromosomes_are_yours_or_if_you_stole/.

⁵ See *id.* An individual's genome is made up of genes, which, when expressed, determine some characteristic about that person. See *infra* notes 18–26 and accompanying text.

⁶ Gardner, *supra* note 4.

⁷ See *infra* notes 8–9 and accompanying text.

⁸ See *infra* notes 180–187 and accompanying text.

⁹ See *infra* notes 180–187 and accompanying text.

¹⁰ See *infra* notes 18–33 and accompanying text.

¹¹ See *infra* notes 34–37, 62–92 and accompanying text.

¹² See *infra* notes 38–92 and accompanying text.

¹³ See *infra* notes 93–170 and accompanying text.

¹⁴ See *infra* notes 93–163 and accompanying text.

be any privacy protection in information that a third party would otherwise be able to discern by physically looking at an individual, but any other information should be protected from investigators without a warrant or a court order.¹⁵ This Note concludes that either legislation needs to be passed to prevent investigators from infringing the genetic privacy rights of individuals, or courts need to start protecting private medical data in genetic material.¹⁶ If new legislation is passed, this Note argues that it should focus on restricting investigatory procedures and the retention of genetic samples after they have been analyzed to prevent the unauthorized use of private genetic information.¹⁷

I. GENETIC MATERIAL: HOW IT IS USED IN A CRIMINAL CONTEXT

A. DNA: What Is It?

Deoxyribonucleic acid (DNA) is the molecule that provides the genetic blueprint for the human body and its processes.¹⁸ DNA consists of a string of chemicals called nucleotides.¹⁹ These nucleotides each contain one of four bases: adenine, guanine, cytosine, or thymine.²⁰ The order of these bases in a strand of DNA forms the genetic code of an organism.²¹ DNA serves as the code that provides instructions for responses to internal and external stimuli.²²

Along certain stretches of DNA, the sequences of these bases, called genes, contain instructions for making proteins.²³ Proteins form the structural components of cells, tissue, and the enzymes that control biochemical reactions, including the functioning of the genes themselves.²⁴ Stretches of DNA that do not code for proteins are often called “junk DNA,” and may perform other functions, such as containing instructions for when certain genes are expressed.²⁵ In fact, recent re-

¹⁵ See *infra* notes 174–240 and accompanying text.

¹⁶ See *infra* notes 174–254 and accompanying text.

¹⁷ See *infra* notes 174–254 and accompanying text.

¹⁸ ANDREWS ET AL., *supra* note 2, at 17.

¹⁹ *Id.*

²⁰ KRIMSKY & SIMONCELLI, *supra* note 1, at 4.

²¹ *Id.*

²² *Id.* at 5.

²³ ANDREWS ET AL., *supra* note 2, at 22.

²⁴ *Id.*

²⁵ *Id.*

search has concluded that this “junk DNA” plays a critical role in controlling how cells, organs, and other tissues behave.²⁶

The International Human Genome Sequencing Consortium predicts that there are between twenty and twenty-five thousand protein-coding genes within a human genome, whereas other groups have predicted larger numbers.²⁷ These protein-coding genes only account for a small percentage of human DNA, as it is estimated that ninety-seven to ninety-eight percent of human DNA consists of “junk DNA.”²⁸

Although humans tend to have genes that perform the same function, differences in the construction of each person’s genes cause them to be expressed differently in different people.²⁹ Different versions of the same gene among different individuals are called alleles.³⁰ Alleles not only help determine whether someone has a genetic predisposition toward certain diseases, but they also account for the visible differences between people such as eye color, skin color, and other physical characteristics.³¹ These alleles are called a person’s genotype, and the observable characteristics that are produced by differences in an individual’s genotype, or these different alleles, are called one’s phenotype.³² Only 0.1% of DNA, or about three million bases, account for the genetic variation that dictates the differences between any two humans.³³

In 2003, the National Human Genome Research Institute (NHGRI) launched a public research consortium called the Encyclopedia of DNA Elements (ENCODE) to identify all functional elements in the human genome sequence, which would allow scientists to understand what causes the differences between humans.³⁴ After successfully testing a one percent portion of the genome, the NHGRI funded awards in 2007 to test the entire human genome.³⁵ The increasing speed of computers

²⁶ Gina Kolata, *Bits of Mystery DNA, Far From ‘Junk,’ Play Crucial Role*, N.Y. TIMES, Sept. 5, 2012, <http://www.nytimes.com/2012/09/06/science/far-from-junk-dna-dark-matter-proves-crucial-to-health.html>. This information can be linked to a wide range of human diseases (e.g., multiple sclerosis, lupus, rheumatoid arthritis, Crohn’s disease, celiac disease) and physical traits like height. *Id.*

²⁷ KRIMSKY & SIMONCELLI, *supra* note 1, at 8.

²⁸ *Id.* at 8–9; Kolata, *supra* note 26. Even this “junk DNA” can provide important information about an individual. Kolata, *supra* note 26.

²⁹ ANDREWS ET AL., *supra* note 2, at 23–24.

³⁰ *Id.*

³¹ *Id.*

³² Sandor, *supra* note 1, at 27 n.14.

³³ KRIMSKY & SIMONCELLI, *supra* note 1, at 9.

³⁴ *The ENCODE Project: ENCYClopedia of DNA Elements*, NAT’L HUM. GENOME RES. INST., <http://www.genome.gov/10005107>.

³⁵ The ENCODE Project Consortium, *A User’s Guide to the Encyclopedia of DNA Elements (ENCODE)*, PLoS BIOL, at e1001046 (Apr. 19, 2011), <http://www.genome.gov/Pages/Re>

and advancing testing technologies will likely soon facilitate a test that can sequence an entire genome within one day for under one thousand dollars.³⁶ As a result, the day in which routinely shed DNA can be replicated and sequenced in order to provide a complete physical and medical profile of a suspect or a witness in a criminal investigation is quickly approaching.³⁷

B. Past and Current Uses of DNA in a Crime Scene Context

1. DNA Fingerprinting

With its currently limited sequencing capabilities, DNA testing serves two main purposes in the criminal context: catching criminals and deterring future criminals.³⁸ In 1997, the FBI and a team of forensic scientists decided that a sequence of thirteen different alleles of “junk DNA” would constitute an individual’s “DNA fingerprint.”³⁹ In choosing these thirteen alleles, a conscious effort was made to avoid any sequence that had known phenotypic properties or that disclosed ancestral origins.⁴⁰ These DNA fingerprints can be used to confirm whether a suspect was present at the scene of the crime, and often these DNA fingerprints are put into a database where police can search for matches with the DNA fingerprint found at a given crime scene.⁴¹ Re-

search/ENCODE/ENCODE_UsersGuide.pdf; Nat’l ENCODE Pilot Project, NAT’L HUM. GENOME RES. INST., <http://www.genome.gov/26525202>.

³⁶ *Archon Genomics XPrize*, ARCHON GENOMICS, <http://genomics.xprize.org>. The XPrize is a competition, starting in 2013, that will award ten million dollars to the first group to sequence 100 genomes of people over the age of 100 accurately, quickly (in under one day), and for under \$1000 per genome sequencing. *Id.*

³⁷ *See id.*; *infra* note 43 and accompanying text (noting that a person’s entire genome can be uncovered from a single small DNA sample left at a crime scene).

³⁸ Etzioni, *supra* note 3, at 200–01.

³⁹ KRIMSKY & SIMONCELLI, *supra* note 1, at 18. The scientists purposely picked “junk DNA” because, at the time, such “junk DNA” could not be used to uncover private information about an individual, such as medical predisposition toward diseases or information that could be used for racial or criminal profiling. *See id.* As science uncovers more information about the “junk DNA” used in these DNA fingerprints, there is the potential that private information could be uncovered from this DNA. *See* Kolata, *supra* note 26.

⁴⁰ KRIMSKY & SIMONCELLI, *supra* note 1, at 95; Melba Newsome, *The Inconvenient Science of Racial DNA Profiling*, WIRED (Oct. 5, 2007), <http://www.wired.com/science/discoveries/news/2007/10/dnprint>.

⁴¹ Edward J. Imwinkelried, *The Relative Priority That Should Be Assigned to Trial Stage DNA Issues*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE, *supra* note 3, at 91, 94–95.

cently, warrants have even been issued using an unknown individual's genetic sequence to help solve crimes.⁴²

Due to a scientific process called Polymerase Chain Reaction (PCR), a person's entire genome can be uncovered from just a small DNA sample left at a crime scene, which may deter criminals by increasing the likelihood of their capture.⁴³ PCR involves replicating tiny segments of an individual's DNA through chemical copying.⁴⁴ As more and more DNA is copied, a sufficient quantity is eventually made for analysis.⁴⁵ Because DNA is much more durable and lasts longer than antigens, enzymes, or proteins, and because DNA tests can be performed on very small sample amounts, DNA fingerprinting is more reliable than the traditional methods of identifying a person, such as eyewitness testimony.⁴⁶ Thus, PCR allows scientists to produce an entire genome even from a stray hair or some skin cells, which may deter criminals by increasing the likelihood of capture.⁴⁷

2. Storage of DNA Fingerprints and DNA Samples in DNA Databases

In 1994, to facilitate the storage and use of DNA fingerprints, Congress passed the DNA Identification Act as part of the Violent Crime Control and Law Enforcement Act.⁴⁸ The DNA Identification Act authorized the FBI to establish and maintain the Combined DNA Index System (CODIS), a software database that allows the sharing of DNA fingerprints uploaded at local, state, and federal levels.⁴⁹ To this day, the seven million DNA profiles in CODIS are frequently subjected to suspicionless searches against unsolved crime scene DNA profiles.⁵⁰

⁴² *Id.*

⁴³ KRIMSKY & SIMONCELLI, *supra* note 1, at 14.

⁴⁴ *Id.*

⁴⁵ *Id.* at 14–15.

⁴⁶ Jordan Garrison, *Courts Face the Exciting and the Inevitable: DNA in Civil Trials*, 23 REV. LITIG. 435, 439–40 (2004).

⁴⁷ See KRIMSKY & SIMONCELLI, *supra* note 1, at 14; Etzioni, *supra* note 3, at 200–01.

⁴⁸ Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-332, 108 Stat. 1796 (codified as amended at 42 U.S.C. §§ 14131–14136e (2006)); KRIMSKY & SIMONCELLI, *supra* note 1, at 29.

⁴⁹ DNA Identification Act of 1994, 42 U.S.C. § 14132 (2006); KRIMSKY & SIMONCELLI, *supra* note 1, at 29. Under the DNA Identification Act of 1994, the director of the FBI was authorized to establish an index of DNA identification records of persons convicted of crimes, analyses of DNA samples recovered from crime scenes, and analyses of DNA samples recovered from unidentified human remains. DNA Identification Act of 1994, Pub. L. No. 103-322, § 210304, 108 Stat. 2065, 2069 (1994).

⁵⁰ KRIMSKY & SIMONCELLI, *supra* note 1, at 236.

By 1998, all fifty states had authorized their own criminal DNA fingerprint databases, and by 2004 all fifty state databases were linked together by CODIS, which allows users in one state to search DNA fingerprints uploaded in any of the other states.⁵¹ In 2000, Congress passed the DNA Analysis Backlog Elimination Act to help populate these databases by requiring the collection of DNA from individuals in custody and on probation, parole, or supervised release who had been convicted of any “qualifying federal offense,” usually a violent crime.⁵² In 2005 the databases were expanded by the Violence Against Women and Department of Justice Reauthorization Act, which authorized the U.S. Attorney General to require, through regulation and without a warrant, DNA to be collected from anyone arrested in the United States or from non-U.S. citizens detained under federal authority.⁵³ On December 10, 2008, the U.S. Department of Justice issued a final rule to implement the DNA Fingerprint Act of 2005, which granted any federal agency with authority to take fingerprints the authority to collect DNA.⁵⁴ This rule expanded DNA collection to arrestees, a practice that only thirteen states had permitted before the rule’s January 2009 effective date.⁵⁵

Although CODIS procedures are dictated by the DNA Identification Act, which states that CODIS contain only the thirteen genes defined by the DNA fingerprint standard, each state has its own DNA databases and procedures governing the use of the genetic information in these DNA databases.⁵⁶ Although the common procedure is for investi-

⁵¹ *Id.* at 29; *Combined DNA Index System*, FED. BUREAU INVESTIGATION, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis> (last visited Feb. 4, 2013).

⁵² DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106-546, § 3, 114 Stat. 2726, 2728–30 (codified as amended at 42 U.S.C. § 14135a); KRIMSKY & SIMONCELLI, *supra* note 1, at 33. In 2001, the USA Patriot Act expanded “qualifying Federal offenses” to include any federal crime of terrorism (listed in 18 U.S.C. 2332b(g)(5)(B) as “any crime of violence,” and “any attempt or conspiracy to commit any of the above offenses”). USA Patriot Act, Pub. L. No. 107-56, § 503, 115 Stat. 272, 364 (2001). “Qualifying Federal offenses” was once again expanded in 2004 to include any felony, any sex-abuse crime (under Chapter 109A or Title 18), any crime of violence, and any attempt to commit any of the above. Justice for All Act, Pub. L. No. 108-405, § 203, 118 Stat. 2260, 2270 (2004).

⁵³ Violence Against Women and Department of Justice Reauthorization Act of 2005, 42 U.S.C. § 14135a (2006); KRIMSKY & SIMONCELLI, *supra* note 1, at 33.

⁵⁴ DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. 74,932, 74,932–43 (Dec. 10, 2008); KRIMSKY & SIMONCELLI, *supra* note 1, at 35.

⁵⁵ DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. at 74,935; KRIMSKY & SIMONCELLI, *supra* note 1, at 36.

⁵⁶ KRIMSKY & SIMONCELLI, *supra* note 1, at 36; *see* DNA Identification Act of 1994, 42 U.S.C. § 14132(a) (2006).

gators to compare the DNA fingerprints obtained at crime scenes to those found in the database, some states have procedures that also include the storage of actual DNA samples.⁵⁷ State databases are linked together through CODIS.⁵⁸ Only eight states expressly prohibit the use of the DNA profiles in the databases to obtain information about human physical traits, predisposition to disease, or medical or genetic disorders.⁵⁹ Some states only allow the data to be used for undefined law enforcement purposes.⁶⁰ Because all states' databases are linked together through CODIS, this Note argues that uniform privacy regulation is more practical than a state-by-state approach.⁶¹

C. Potential Future Uses of DNA in Crime Scenes

There are four main ways in which DNA sequencing either has been tried or theoretically could be tried to help solve crimes: forensic DNA phenotyping, ancestral genotyping, behavioral genotyping and profiling, and medical phenotyping.⁶² Each of these methods could help solve crimes, but each also requires strict regulation to guard against abuse.⁶³

⁵⁷ KRIMSKY & SIMONCELLI, *supra* note 1, at 36–37.

⁵⁸ *Combined DNA Index System*, FED. BUREAU INVESTIGATION, *supra* note 51.

⁵⁹ KRIMSKY & SIMONCELLI, *supra* note 1, at 238; Seth Axelrad, *Use of Forensic DNA Database Information for Medical or Genetic Research*, AM. SOC'Y L. MED. & ETHICS (2005), http://www.aslme.org/dna_04/reports/axelrad3.pdf. The states that expressly prohibit the use of DNA databases to obtain information on physical traits, predispositions to disease, or medical or genetic disorders are Indiana, Rhode Island, South Dakota, Texas, Utah, Vermont, and Wyoming. Axelrad, *supra*.

⁶⁰ KRIMSKY & SIMONCELLI, *supra* note 1, at 238; Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK L. REV. 127, 156 (2001). For instance, in 1996, the year before Massachusetts enacted a law authorizing its own state DNA database, the Massachusetts legislature commissioned a study to research the "biological cause of crime," which it considered a valid law enforcement purpose. Barry Steinhardt, *Privacy and Forensic DNA Data Banks*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE, *supra* note 3, at 175, 184–85; Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309, 336 (2010). For a table of states and their respective DNA Databank statutes, see Davina Dana Bressler, Note, *Criminal DNA Databank Statutes and Medical Research*, 43 JURIMETRICS J. 51, 68–70 (2002).

⁶¹ See *Combined DNA Index System*, FED. BUREAU INVESTIGATION, *supra* note 51; *infra* notes 241–254 and accompanying text. There also is a concern that states may create new functions for these databases, and that these new functions may violate the privacy rights of individuals. See Tania Simoncelli & Barry Steinhardt, *California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases*, 34 J.L. MED. & ETHICS 199, 203 (2006).

⁶² See *infra* notes 64–92 and accompanying text.

⁶³ See *infra* notes 64–92 and accompanying text.

1. Forensic DNA Phenotyping

With forensic DNA phenotyping, forensic scientists can analyze DNA from a crime scene to determine an individual's physical characteristics, or phenotype.⁶⁴ For instance, with processes like PCR, scientists can take a small amount of genetic material left behind by a perpetrator at a crime scene, such as hair, skin flakes, or semen, and decode the perpetrator's genome.⁶⁵ As scientists continue to learn more about the relationships between an individual's genotype and that person's phenotype, the physical traits of an individual will be readily uncovered by decoding one's genotype.⁶⁶ Indeed, scientists can already determine an individual's hair color, eye color, and ethnic background.⁶⁷ As future research reveals more correlations between genotype and phenotype, law enforcement personnel will someday be able to use DNA to create a probabilistic model of the perpetrator's appearance, allowing law enforcement to narrow lists of suspects and to operate more efficiently.⁶⁸

Notwithstanding that forensic DNA phenotyping requires more research into the expression of genes in individuals' appearances, critics argue that this correlation between phenotypes and their underlying genotypes would not significantly aid law enforcement personnel.⁶⁹ Critics argue that many physical characteristics, such as hair color, eye color, and even body type, can be changed with modern technology such as plastic surgery, and that the use of phenotyping might start a slippery slope toward eugenics.⁷⁰

2. Ancestral Genotyping

Some alleles only appear in certain ethnic populations, allowing an individual's genome to be used to reveal their heritage.⁷¹ Although

⁶⁴ KRIMSKY & SIMONCELLI, *supra* note 1, at 90.

⁶⁵ *See id.*

⁶⁶ *Id.*

⁶⁷ Newsome, *supra* note 40.

⁶⁸ *See id.*

⁶⁹ KRIMSKY & SIMONCELLI, *supra* note 1, at 102; Bert-Jaap Koops & Maurice Schellekens, *Forensic DNA Phenotyping: Regulatory Issues*, 9 COLUM. SCI. & TECH. L. REV. 158, 164–65 (2008).

⁷⁰ *See* KRIMSKY & SIMONCELLI, *supra* note 1, at 102; Koops & Schellekens, *supra* note 69, at 164–65, 196–98. The discovery of aggression-related genes or connections between physical features like albinism and a predisposition toward crime, for example, could be used to discriminate against those who are unfortunate enough to have such genes. Koops & Schellekens, *supra* note 69, at 196–98. This genetic discrimination might inflict such hardship on carriers of particular genetic traits that the traits would eventually be removed from the gene pool. *Id.*

⁷¹ KRIMSKY & SIMONCELLI, *supra* note 1, at 91–93.

there is actually more genetic variation within ethnic and racial groups than between them, scientists have been able to uncover differences between groups that can allow them to predict the probable ethnic background of an individual.⁷² In a Louisiana investigation involving a serial killer, police, based on eyewitness testimony, found themselves looking for a white killer who drove a white truck.⁷³ A company called DNAPrint Genomics offered to test DNA from the crime scenes, and it determined that the perpetrator had an 85% sub-Saharan African and 15% Native American heritage.⁷⁴ As a result of this ancestral genotyping, the police were able to change the direction of their investigation and find the serial killer.⁷⁵ Although ancestral genotyping is similar to forensic DNA phenotyping, it is mostly used for racial and ethnic profiling.⁷⁶ Despite the fact that critics may disapprove of this technique, supporters argue that it is no different than narrowing the search for a perpetrator of a given race based on eyewitness testimony.⁷⁷

A related form of ancestral genotyping is familial searching, which is helpful when a suspect's DNA fingerprint cannot be obtained or is not in a database.⁷⁸ For example, law enforcement may employ familial searching by using DNA databases to locate possible relatives of the perpetrators of a crime and then interview those relatives to ascertain either the suspect's location or guilt.⁷⁹ Familial searching may also be used to obtain a suspect's DNA indirectly by analyzing DNA from his family members.⁸⁰ Both of these techniques have significant implications for the genetic privacy of potentially innocent people who share close matches to suspects' DNA profiles, because such testing may uncover private information about these individuals even though they are not suspected of any wrongdoing.⁸¹

⁷² *Id.* at 91.

⁷³ *Id.* at 92–93.

⁷⁴ *Id.* at 93.

⁷⁵ *Id.*

⁷⁶ *See id.* at 91–93.

⁷⁷ *See* Koops & Schellekens, *supra* note 69, at 183 (discussing the debate between supporters and critics of ancestral genotyping).

⁷⁸ *See* Suter, *supra* note 60, at 318–19.

⁷⁹ *Id.*

⁸⁰ Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34 J.L. MED. & ETHICS 153, 156 (2006).

⁸¹ *See* Suter, *supra* note 60, at 342–52.

3. Behavioral Genotyping and Profiling

Behavioral genotyping and profiling seeks to find correlations between an individual's genome and criminal behavior.⁸² Finding such links would allow police to focus investigations on those genetically predisposed to engage in deviant behavior like pedophilia, rape, or acts of aggression.⁸³ In 1965, a study published in *Nature* found that "dangerously violent" inmates in an Edinburgh, Scotland prison hospital had an extra Y chromosome as compared to the general population.⁸⁴ Although this study lacked a satisfactory control group, another study in 2002, published in *Science*, had more merit.⁸⁵ In this study, researchers discovered a genetic marker linked to violent behavior.⁸⁶ Although the use of psychotropic drugs might mitigate the effects of the expression of these genes, and although this material should not be used to predict future crimes, a genetic predisposition to aggression could be useful in directing an investigation in the future.⁸⁷

4. Medical Phenotyping

Medical phenotyping consists of decoding an individual's genome to determine that individual's disposition to certain diseases.⁸⁸ The idea behind medical phenotyping is that, if there were a positive result for a disease that required medical treatment, police could track down potential suspects from hospital or pharmacy records.⁸⁹ Currently, federal law would allow such an inquiry as long as the police have probable cause that an individual may have committed a crime, allowing a warrant to be obtained for access to medical records.⁹⁰ Medical phenotyping also raises serious privacy concerns, namely an individual's right to know or not know about a medical condition.⁹¹ Critics argue that such disclosures should not be influenced by police investigations, because no significant

⁸² KRIMSKY & SIMONCELLI, *supra* note 1, at 96.

⁸³ *Id.*

⁸⁴ *Id.*; Patricia A. Jacobs et al., *Aggressive Behavior, Mental Sub-normality and the XYY Male*, 208 NATURE 1351, 1351-52 (1965). The study found that 7 of 197 inmates were XXY, whereas the ratio of XYY in the general population was 1.3 out of every 1000 people. Jacobs et al., *supra*, at 1351-52.

⁸⁵ KRIMSKY & SIMONCELLI, *supra* note 1, at 97; see Avshalom Caspi et al., *Role of Genotype in the Cycle of Violence of Maltreated Children*, 297 SCIENCE 851, 851-54 (2002).

⁸⁶ KRIMSKY & SIMONCELLI, *supra* note 1, at 97; see Caspi et al., *supra* note 85, at 851-54.

⁸⁷ See KRIMSKY & SIMONCELLI, *supra* note 1, at 97-98.

⁸⁸ *Id.* at 98.

⁸⁹ *Id.*

⁹⁰ *Id.* at 100.

⁹¹ Koops & Schellekens, *supra* note 69, at 175, 180-81.

governmental interest outweighs the invasion of an individual's right to know his or her own medical predisposition to disease.⁹²

II. PRIVACY RIGHTS IN DNA

This Part analyzes the privacy rights in genetic material.⁹³ Section A details the formation and courts' initial interpretations of privacy rights.⁹⁴ Section B analyzes courts' attempts to apply these interpretations to cases involving genetic information.⁹⁵ Section C focuses on the growing academic consensus that genetic privacy legislation must be enacted.⁹⁶ Within this framework, Section D details the current lack of protection for private information contained in crime scene DNA.⁹⁷

A. Privacy According to the Courts

The word privacy was not prevalent in law until Samuel Warren and Louis Brandeis published an influential *Harvard Law Review* article outlining a "right to privacy" that served as the foundation for future privacy jurisprudence.⁹⁸ Privacy is not mentioned in the Constitution, but in 1965 the U.S. Supreme Court expressly recognized a constitutional right to privacy in *Griswold v. Connecticut*, though the Court located it within the penumbras of various amendments composing the Bill of Rights.⁹⁹ In 1967, in *Katz v. United States*, the U.S. Supreme Court addressed the right to privacy within the Fourth Amendment, which protects citizens from unreasonable searches and seizures.¹⁰⁰ Although a right to privacy is not expressly mentioned in the Constitution, some states have included provisions in their own constitutions explicitly providing a right to privacy, and courts since *Katz* have focused privacy ju-

⁹² *Id.*

⁹³ See *infra* notes 98–173 and accompanying text.

⁹⁴ See *infra* notes 98–110 and accompanying text.

⁹⁵ See *infra* notes 111–163 and accompanying text.

⁹⁶ See *infra* notes 164–170 and accompanying text.

⁹⁷ See *infra* notes 171–173 and accompanying text.

⁹⁸ KRIMSKY & SIMONCELLI, *supra* note 1, at 226; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890).

⁹⁹ 381 U.S. 479, 481–86 (1965); KRIMSKY & SIMONCELLI, *supra* note 1, at 226. Locating the right to privacy within the penumbras of the Amendments means that the Amendments imply that a generalized right to privacy exists. *Griswold*, 381 U.S. at 484.

¹⁰⁰ 389 U.S. 347, 351–53 (1967). The Fourth Amendment expressly protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," but recognizes that searches of these areas may occur when warrants are issued "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

risprudence on either state constitutional provisions or the Fourth Amendment.¹⁰¹

Justice Harlan's concurrence in *Katz* provides the controlling test for determining whether government action constitutes a Fourth Amendment search.¹⁰² In *Katz*, the police were listening to an individual's telephone conversations in a public telephone booth without a warrant.¹⁰³ The Court recognized that what a person knowingly exposes to the public, even in his or her own home or office, does not receive Fourth Amendment protection.¹⁰⁴ But what he or she seeks to preserve as private, even in an area accessible to the public, such as a telephone call in a public telephone booth, may be constitutionally protected.¹⁰⁵ Justice Harlan stated in his concurrence that, to invade an individual's privacy, a person must have exhibited an actual, subjective expectation of privacy, and that this expectation must be one that society is willing to recognize as reasonable.¹⁰⁶

Justice Harlan's test was adopted and later applied in decisions, such as *California v. Greenwood* in 1988, where the U.S. Supreme Court addressed the expectation of privacy protected by the Fourth Amendment.¹⁰⁷ In *Greenwood*, the Court held that, because the plaintiff deposited his trash on the side of his street in an area particularly suited for public inspection and for the express purpose of having strangers take it, the plaintiff had no reasonable expectation of privacy in the inculpatory items that he discarded and that the police acquired without a warrant.¹⁰⁸

In 2001, the U.S. Supreme Court acknowledged the tension between advancing technology and reasonable expectations of privacy in *Kyllo v. United States*, where police used a thermal scanner without a war-

¹⁰¹ See, e.g., CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."); see also KRIMSKY & SIMONCELLI, *supra* note 1, at 226 (noting the existence of these more extensive state constitutional provisions).

¹⁰² 389 U.S. at 361 (Harlan, J., concurring); KRIMSKY & SIMONCELLI, *supra* note 1, at 242.

¹⁰³ *Katz*, 389 U.S. at 348.

¹⁰⁴ *Id.* at 351–52.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 361 (Harlan, J., concurring).

¹⁰⁷ 486 U.S. 35, 39 (1988).

¹⁰⁸ *Id.* at 40–41.

rant to discover that a man was growing drugs in his house.¹⁰⁹ In *Kyllo*, the Court held that the use of technology not in general public use to obtain information that could not otherwise have been obtained without “physical intrusion into a constitutionally protected area” violates the reasonable expectation of privacy protected by the Fourth Amendment.¹¹⁰

B. *Privacy as Applied to Genetic Information*

The genetic privacy case law following *Katz* has focused on two main types of warrantless searches: those involving mandatory intrusions into a person’s body and those that involve taking an individual’s sensitive information without that person’s knowledge.¹¹¹ In addition, the courts have created uncertainty as to (1) whether the genetic material left at a crime scene has been abandoned, thus extinguishing an individual’s privacy right in the material, and (2) how the storage of genetic information in DNA databases affects an individual’s right to privacy.¹¹²

1. Mandatory Intrusions

Mandatory intrusions consist of a forced seizure of genetic material from an individual without a warrant.¹¹³ The function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the state.¹¹⁴ By requiring a warrant before law enforcement personnel can force an individual to provide genetic infor-

¹⁰⁹ See 533 U.S. 27, 29–30 (2001).

¹¹⁰ *Id.* at 34–35, 40. In 2012 the U.S. Supreme Court again considered these privacy rights in *United States v. Jones*, but was split on how to treat the *Katz* test in a situation that implicated trespass onto an individual’s property. 132 S. Ct. 945, 953 (2012). In *Jones*, four justices stated that placing a GPS monitoring device on a car was a “search” that required a warrant, and that the *Katz* test was not necessarily implicated in such a trespass. *Id.* at 949, 952. Four justices stated that a “search” did not occur, and that the *Katz* test supplanted traditional search and seizure analysis, which only required the demonstration that a technical trespass is sufficient to show a search. *Id.* at 958–59 (Alito, J., concurring). In the end, although it is unclear to what extent the *Katz* test should be applied to intrusions on property rights, *Jones* affirmed the *Katz* test for governmental intrusions on non-property privacy rights. See *id.* at 953, 958–59 (Alito, J., concurring).

¹¹¹ See *infra* notes 113–135 and accompanying text.

¹¹² See *infra* notes 136–163 and accompanying text.

¹¹³ See *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 616 (1989); *Schmerber v. California*, 384 U.S. 757, 767–68 (1966).

¹¹⁴ *Schmerber*, 384 U.S. at 767.

mation, the Fourth Amendment ensures that a neutral magistrate will determine whether this intrusion is justified.¹¹⁵

In 1966 in *Schmerber v. California*, the U.S. Supreme Court concluded that a warrantless blood test was reasonable because delaying the test might defeat its purpose and the test was performed in a reasonable manner.¹¹⁶ In this case, an individual was arrested after an accident for driving under the influence and, while he was in the hospital, a blood test was taken to test for alcohol.¹¹⁷ The issue was whether a warrant was needed for this blood test, which was used to convict the driver.¹¹⁸ Despite upholding the validity of the test, the Court recognized in dicta that the Constitution does not forbid the states' minor intrusions into an individual's body under stringently limited conditions.¹¹⁹ Yet the Court noted that more substantial intrusions, or intrusions under other conditions, would not be reasonable.¹²⁰

In 1989 in *Skinner v. Railway Labor Executives' Ass'n*, the U.S. Supreme Court recognized that a compelled intrusion into the body constitutes a search, but the reasonableness of this search is judged by "balancing [the] intrusion on the individual's Fourth Amendment interests against [the practice's] promotion of legitimate governmental interests."¹²¹ The Court had to decide whether the Federal Railroad Administration's regulations were valid in testing railway employees for drugs and alcohol.¹²² One of the challenged rules required the collection of blood and urine samples for testing after any collision that resulted in a reportable injury or damage to railroad property of over fifty-thousand dollars.¹²³ The Court held that, because of the special needs in such a scenario to determine whether a railroad worker was intoxicated, the physical intrusion of taking blood from railroad workers was reasonable under the Fourth Amendment.¹²⁴ The Court did

¹¹⁵ See *Skinner*, 489 U.S. at 622.

¹¹⁶ 384 U.S. at 770–71.

¹¹⁷ *Id.* at 758–59.

¹¹⁸ *Id.* at 770.

¹¹⁹ *Id.* at 772.

¹²⁰ *Id.* ("That we today hold that the Constitution does not forbid the States minor intrusions into an individual's body under stringently limited conditions in no way indicates that it permits more substantial intrusions, or intrusions under other conditions.")

¹²¹ 489 U.S. at 619 (citing *Delaware v. Prouse*, 440 U.S. 648, 654 (1979)).

¹²² *Id.* at 606.

¹²³ *Id.*

¹²⁴ *Id.* at 623–24. The Court reasoned that because alcohol and other drugs are eliminated from the bloodstream at a constant rate, the burden of getting a warrant would frustrate the governmental purpose of the search. See *id.* at 623. In the time it would take to obtain the warrant, the test would no longer be an accurate depiction of the individual's

require, however, that the warrantless search be based on probable cause.¹²⁵

2. Taking Sensitive Information Without Knowledge

As opposed to challenging the forced seizure of genetic information, the second line of challenges to the use of genetic material involves the use of tests that reveal an individual's private, sensitive information without a warrant.¹²⁶ Because medical information is the type of information in which one enjoys the highest expectation of privacy, the search of this information without a warrant or a prevailing governmental interest that outweighs an individual's privacy interest constitutes an unreasonable search.¹²⁷

In 1998 in *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, the U.S. Court of Appeals for the Ninth Circuit held that unauthorized tests that reveal highly sensitive medical facts are Fourth Amendment searches.¹²⁸ In this case, employees of a state and federal research facility were, without their knowledge, tested for highly private and sensitive medical information, such as syphilis, sickle cell anemia, and pregnancy.¹²⁹ The court held that these tests could be considered Fourth Amendment searches because individuals have the highest expectation of privacy in sensitive medical information.¹³⁰ Yet, the court recognized that there would be no violation of privacy rights if the testing was authorized, or if the plaintiffs reasonably should have known that the blood and urine samples they provided would be used for the disputed testing and failed to object.¹³¹

Unlike *Norman-Bloodsaw*, in 2007 the Washington Supreme Court in *State v. Athan* concluded that individuals do not have an expectation of privacy in discarded DNA.¹³² In *Athan*, the court considered whether the

intoxication at the time of the accident. *See id.* Thus, the Court recognized that the "special needs" of this kind of scenario may make the warrant procedures impracticable. *See id.* at 619, 623.

¹²⁵ *Id.* at 624.

¹²⁶ *See Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1268–70 (9th Cir. 1998); *State v. Athan*, 158 P.3d 27, 31–32 (Wash. 2007).

¹²⁷ *Id.* at 1269–70; *see Katz*, 389 U.S. at 361 (Harlan, J., concurring).

¹²⁸ *See Norman-Bloodsaw*, 135 F.3d at 1268–70. Although the court so held, it remanded in this case because material issues of fact existed as to whether the tests were authorized and whether the plaintiffs reasonably should have known that the blood and urine samples they provided would be used for the disputed testing and failed to object. *Id.* at 1270.

¹²⁹ *Id.* at 1269–70.

¹³⁰ *Id.*

¹³¹ *Id.* at 1270.

¹³² *See Athan*, 158 P.3d at 37.

defendant had a privacy interest in the DNA located in saliva on an envelope he placed in the mail, which was used to connect him to a crime that had occurred twenty years earlier.¹³³ The court held that there is no subjective expectation of privacy in discarded genetic material, just as there is no subjective expectation of privacy in fingerprints or footprints left in a public place.¹³⁴ As a result, the court upheld the constitutionality of the warrantless search, both under the Fourth Amendment and the Washington Constitution, which has been interpreted to provide greater protection than the Fourth Amendment.¹³⁵

3. Abandoned or Relinquished Property Extinguishes Privacy Rights?

An important implication of *Athan* is the idea that the privacy interest in discarded genetic material is extinguished when the material has been abandoned or relinquished.¹³⁶ When police acquire DNA from a suspect, they often argue that such genetic material has been “abandoned” and, as a result, that the individual who “abandons” his or her DNA no longer has any privacy interest in it or the information it holds.¹³⁷ Sometimes police have acquired DNA by offering an individual a cigarette or a drink during interrogation and collecting the items afterward, or they follow the individual around and pick up discarded items for subsequent DNA testing.¹³⁸ The presumption in these situations is that the practice of collecting and analyzing an individual’s DNA without his or her knowledge or consent is legal.¹³⁹

Law enforcement personnel also argue that people have no privacy rights in DNA that has been relinquished in tissue repositories in the United States.¹⁴⁰ This argument invokes *United States v. Miller*, where the U.S. Supreme Court in 1976 held that when a person voluntarily relinquishes checks and deposit slips to a bank, subpoenas requiring the bank to produce these materials do not intrude into any area in which the defendant had a protected Fourth Amendment interest.¹⁴¹

¹³³ *Id.* at 31–32.

¹³⁴ *Id.* at 37.

¹³⁵ *Id.*; KRIMSKY & SIMONCELLI, *supra* note 1, at 112.

¹³⁶ *See* 158 P.3d at 37.

¹³⁷ KRIMSKY & SIMONCELLI, *supra* note 1, at 109.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ D.H. Kaye & Michael E. Smith, *DNA Databases for Law Enforcement: The Coverage Question and the Case for a Population-Wide Database*, in *DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE*, *supra* note 3, at 247, 259.

¹⁴¹ 425 U.S. 435, 440 (1976); Kaye & Smith, *supra* note 140, at 259.

Because we leave our DNA everywhere, the argument that an individual no longer has any privacy interest in abandoned or relinquished DNA has serious implications for personal privacy.¹⁴² With readily available genetic testing services, nothing is stopping ordinary citizens from taking another person's DNA and obtaining some basic private medical information.¹⁴³ Therefore, the idea that abandoned or relinquished DNA has no privacy rights and thus can be completely sequenced without a warrant has troubling consequences for the protection of sensitive medical data, especially as genetic sequencing technology becomes more advanced.¹⁴⁴

4. Legal Challenges to DNA Databases

Although the use of DNA databanks has been challenged in all twelve circuits as an invasion of an individual's privacy, the constitutionality of the system has been upheld, though the nature of an individual's privacy in that information is unclear.¹⁴⁵ The seizure and analysis of DNA is a search subject to the Fourth Amendment.¹⁴⁶ The courts have generally judged that the mandatory collection of DNA from convicted felons without any warrant or further probable cause is not an "unreasonable search" in violation of the Fourth Amendment.¹⁴⁷

¹⁴² See Gardner, *supra* note 4.

¹⁴³ See *id.* For example, the company 23andMe indicates susceptibility to genetic diseases and medical conditions. 23ANDME, <http://www.23andme.com> (last visited on Feb. 12, 2013). 23andMe allows consumers to mail in a tube of saliva, which is then partially sequenced in order to provide the consumer with ancestry information and potential health risks. *Id.*

¹⁴⁴ See Koops & Schellekens, *supra* note 69, at 175, 180–81; Gardner, *supra* note 4.

¹⁴⁵ KRIMSKY & SIMONCELLI, *supra* note 1, at 244–45; see, e.g., *Wilson v. Collins*, 517 F.3d 421, 428 (6th Cir. 2008) (upholding the constitutionality of DNA databanks); *United States v. Kriesel*, 508 F.3d 941, 950 (9th Cir. 2007) (same); *United States v. Weikert*, 504 F.3d 1, 14 (1st Cir. 2007) (same); *United States v. Banks*, 490 F.3d 1178, 1193 (10th Cir. 2007) (same); *United States v. Amerson*, 483 F.3d 73, 89 (2d Cir. 2007) (same); *United States v. Hook*, 471 F.3d 766, 773 (7th Cir. 2006) (same); *United States v. Kraklio*, 451 F.3d 922, 924–25 (8th Cir. 2006) (same).

¹⁴⁶ *Schmerber*, 384 U.S. at 767.

¹⁴⁷ KRIMSKY & SIMONCELLI, *supra* note 1, at 244–45. The Second, Seventh, and Tenth circuits have followed the U.S. Supreme Court's 1989 decision in *Skinner v. Railway Labor Executives' Ass'n* by applying a "special needs" exception, which states that although individualized suspicion is generally required for a search, when a search serves a special need distinguishable from ordinary law-enforcement needs, such as using a DNA database to assist in solving crimes, this interest outweighs the privacy interest of those previously convicted of crimes. 489 U.S. at 619–20; see *Hook*, 471 F.3d at 766, 773; *Nicholas v. Goord*, 430 F.3d 652, 667, 672 (2d Cir. 2005); *United States v. Kimler*, 335 F.3d 1132, 1146 (10th Cir. 2003). Other courts have employed a general balancing test and have concluded that parolees and other prisoners under conditional release are not entitled to the full panoply of rights and protections possessed by the general public. *United States v. Sczubelek*, 402 F.3d 175, 184 (3d Cir. 2005);

Although the analysis and inclusion of DNA in a database is a search subject to the protections of the Fourth Amendment, courts have consistently held that accessing stored records in DNA databases is not a Fourth Amendment search.¹⁴⁸ In 2010 in *Boroian v. Mueller*, the U.S. Court of Appeals for the First Circuit observed that the government's use of CODIS to match a plaintiff's profile against other profiles in the database after the plaintiff had finished his probation was limited to a comparison of the identification records already in the government's possession.¹⁴⁹ As a result, these searches did not reveal any new, private, or intimate information about the plaintiff.¹⁵⁰ In addition, the court recognized that the government's comparison of the plaintiff's DNA profile with other profiles in CODIS is exactly what CODIS was initially lawfully created for.¹⁵¹ As a result, the court held that the retention and matching of the plaintiff's profile against other profiles in CODIS did not violate an expectation of privacy that society is prepared to recognize as reasonable, and thus did not constitute a separate search under the Fourth Amendment.¹⁵²

The court in *Boroian* did not address whether DNA in state databases can be used for purposes other than mere identification.¹⁵³ The court refused to hold that, once the DNA sample is lawfully extracted, the individual loses a reasonable expectation of privacy with respect to any subsequent use of that sample.¹⁵⁴ This means that any further use of a DNA profile other than as a comparison to other profiles in a database must satisfy the reasonableness requirement of the Fourth Amendment.¹⁵⁵ As genetic testing becomes less expensive, there could be incentives to test the DNA samples in state databases for, among

Padgett v. Donald, 401 F.3d 1273, 1278, 1282 (11 Cir. 2005); *United States v. Kincade*, 379 F.3d 813, 833 (9th Cir. 2004); *Groceman v. U.S. Dep't of Justice*, 354 F.3d 411, 413–14 (5th Cir. 2004); *Jones v. Murray*, 962 F.2d 302, 307 (4th Cir. 1992).

¹⁴⁸ See *Boroian v. Mueller*, 616 F.3d 60, 68 (1st Cir. 2010); accord *United States v. Mitchell*, 652 F.3d 387, 411 n.21 (3d Cir. 2011); *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir. 2006).

¹⁴⁹ 616 F.3d at 67.

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² *Id.* at 67–68.

¹⁵³ See *id.* at 62–71.

¹⁵⁴ *Id.* at 68–69 (“We do not hold, as some courts have suggested, that once a DNA sample is lawfully extracted from an individual and a DNA profile lawfully created, the individual necessarily loses a reasonable expectation of privacy with respect to any subsequent use of that profile.”).

¹⁵⁵ *Boroian*, 616 F.3d at 68, 71.

other things, genetic predisposition to criminal behavior.¹⁵⁶ Yet, courts have provided no guidance as to what kind of further genetic testing is reasonable.¹⁵⁷ Accordingly, the constitutionality of the use of DNA in CODIS databases for purposes other than mere identification will remain unknown until these tests are actually performed and challenged.¹⁵⁸

DNA samples stored in state databases could be put to a multitude of uses as genetic testing technology advances, including the decoding of an individual's entire genome for research into genetic influences on criminality or profiling of those predisposed to criminal activity.¹⁵⁹ There is no national policy on the retention of physical DNA samples, and in almost every state the physical samples are retained indefinitely.¹⁶⁰ Law enforcement officials want to retain samples so that, as new technology arises, information from retained samples can be included in future databases.¹⁶¹ According to these officials, the retention policies help reduce the cost of populating new databases if the information captured by the databases were to change.¹⁶² This means that an individual's entire genome is likely stored long after any potential incarceration, or even acquittal, occurs, allowing private information to potentially be extracted from a sample regardless of an individual's guilt or rehabilitation.¹⁶³

C. *The Extralegal Debate over Genetic Privacy*

Although the courts have not adopted a uniform stance on genetic privacy, there is a growing consensus among bioethicists, medical pro-

¹⁵⁶ See *supra* notes 82–87 and accompanying text (discussing how the genotypes of criminals could be used to identify individuals who are genetically predisposed to commit future offenses).

¹⁵⁷ See *Boroian*, 616 F.3d at 68, 71; Suter, *supra* note 60, at 331.

¹⁵⁸ See *Boroian*, 616 F.3d at 68, 71; see also *United States v. Karo*, 468 U.S. 705, 712 (1984) (recognizing that the Court has never held that a potential, as opposed to actual, invasion of privacy constitutes a search for the purposes of the Fourth Amendment).

¹⁵⁹ See Suter, *supra* note 60, at 334–35; see *supra* notes 82–87 and accompanying text.

¹⁶⁰ Rothstein & Talbott, *supra* note 80, at 158. Wisconsin is the only state that requires the destruction of all offender samples after analysis is performed, but reportedly no samples have yet been destroyed. WISC. STAT. ANN. § 165.77 (West 2009); see Rothstein & Talbott, *supra* note 80, at 158. Arizona requires that all samples be retained for at least thirty-five years, and Nebraska requires that all samples be permanently retained. ARIZ. REV. STAT. ANN. § 13-610 (2010); NEB. REV. STAT. § 29-4105 (2009).

¹⁶¹ See NAT'L INST. OF JUSTICE, THE FUTURE OF FORENSIC DNA TESTING: PREDICTIONS OF THE RESEARCH AND DEVELOPMENT WORKING GROUP 36 (2000), <https://www.ncjrs.gov/pdffiles1/nij/183697.pdf>.

¹⁶² See *id.*

¹⁶³ See *id.*

professionals, and legislators that an individual has a privacy right in his or her own DNA.¹⁶⁴ Privacy has generally been broken down into four main categories: informational privacy, which consists of having control over highly personal information about ourselves; relational privacy, which consists of privacy in determining with whom we have personal, intimate relationships; privacy in decision making, which consists of the freedom to make decisions for ourselves without being watched or unduly influenced by others; and the right to exclude others from our personal things and places.¹⁶⁵ Most of the legal debate about genetic privacy has focused on the bodily intrusion of obtaining a DNA sample and the Fourth Amendment, but as scientists continue to uncover the function of genes, the legal treatment of informational privacy in personal data in our genome will become an important issue.¹⁶⁶ In the meantime, drawing conclusions about the information within specific genomes before the full significance of this DNA is understood is a struggle for some judges.¹⁶⁷

Some scholars have argued that genetic privacy is better framed as a property matter.¹⁶⁸ The Genetic Privacy Act, an unenacted legislative proposal drafted for the Ethical, Legal, and Social Implications program of the Human Genome Project, provides that individuals own their DNA, and that no one can use an individual's DNA without authorization.¹⁶⁹ As a result, the proponents of the Genetic Privacy Act support individuals having a property right to exclude others from the information contained in their own genome.¹⁷⁰

¹⁶⁴ KRIMSKY & SIMONCELLI, *supra* note 1, at 113; George J. Annas et al., *Guidelines for Protecting Privacy of Information Stored in Genetic Data Banks*, in THE GENETIC PRIVACY ACT AND COMMENTARY (1995), www.ornl.gov/sci/techresources/Human_Genome/resource/privacy/privacy1.html; Press Release, Biotechnology Industry Organization, International Biotechnology Community Supports Genetic Privacy—BIO Seeks White House Support (Jun. 5, 1997), www.bio.org/media/press-release/international-biotechnology-community-supports-genetic-privacy-bio-seeks-white-h.

¹⁶⁵ George J. Annas, *Genetic Privacy*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE, *supra* note 3, at 135, 135.

¹⁶⁶ Viktor Mayer-Schönberger, *Strands of Privacy: DNA Databases, Informational Privacy, and the OECD Guidelines*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE, *supra* note 3, at 225, 226–27; *see supra* notes 113–125 and accompanying text (detailing the legal history covering mandatory bodily intrusions to obtain genetic material).

¹⁶⁷ *Kincade*, 370 F.3d at 850 (Reinhardt, J., dissenting) (arguing that the lack of capacity to comprehend the full significance of the function of DNA in the CODIS databases should not preclude analysis of the privacy implications of the genetic material stored in those databases).

¹⁶⁸ *See* Annas, *supra* note 165, at 139.

¹⁶⁹ *Id.*; Annas et al., *supra* note 164.

¹⁷⁰ *See* Annas et al., *supra* note 164.

D. *Current Crime Scene DNA Privacy Rights (or Lack Thereof)*

Although there is an extralegal consensus that informational privacy should be protected in routinely shed DNA, there is currently no law that regulates or restricts the ways law enforcement can analyze evidence obtained from a crime scene, including blood, tissue, hair, and semen.¹⁷¹ According to the current legal reasoning, individuals do not possess any privacy rights in crime scene evidence.¹⁷² If there were any privacy rights in this DNA, the uncovering of information from this DNA would require a warrant because, according to the Supreme Court, the Fourth Amendment requires deliberate, impartial judgment of a judicial officer to be interposed between a citizen and police when such searches occur.¹⁷³

III. WHAT KIND OF INFORMATION SHOULD BE PROTECTED?

This Part suggests that policies should be enacted to prevent police from uncovering private information in crime scene DNA without a warrant.¹⁷⁴ Section A argues that some genetic information in crime scene DNA should be protected.¹⁷⁵ Section B splits this genetic information into two groups: phenotypic information, which is exposed to the public; and non-phenotypic information, which remains hidden in one's genome.¹⁷⁶ Section C criticizes the argument that non-phenotypic information in crime scene DNA is abandoned.¹⁷⁷ Because non-phenotypic information has not been abandoned and contains private, sensitive medical information, Section D concludes that police should be required by courts or by legislation to obtain a warrant to uncover non-phenotypic data from crime scene DNA.¹⁷⁸ Finally, Section E concludes that states should not be permitted to retain physical DNA samples indefinitely due to the ease with which non-phenotypic data can be revealed from these samples.¹⁷⁹

¹⁷¹ KRIMSKY & SIMONCELLI, *supra* note 1, at 99.

¹⁷² *Id.*

¹⁷³ See *Katz*, 389 U.S. at 357 (quoting *Agnello v. United States*, 269 U.S. 20, 33 (1925)); *Wong Sun v. United States*, 371 U.S. 471, 481–82 (1963)); *supra* notes 93–144 and accompanying text (detailing the judicial interpretation of privacy rights in DNA).

¹⁷⁴ See *infra* notes 180–254 and accompanying text.

¹⁷⁵ See *infra* notes 180–187 and accompanying text.

¹⁷⁶ See *infra* notes 188–210 and accompanying text.

¹⁷⁷ See *infra* notes 211–230 and accompanying text.

¹⁷⁸ See *infra* notes 231–240 and accompanying text.

¹⁷⁹ See *infra* notes 241–254 and accompanying text.

A. *There Should Be Some Protection from Sequencing Public DNA*

There are currently no privacy rights in crime scene DNA.¹⁸⁰ Because this DNA could potentially be used to determine almost anything about a person, and because it already can be used to uncover private medical information such as predisposition to some diseases, decoding information from DNA should be strictly regulated.¹⁸¹ Accordingly, legislation should be enacted to protect the informational privacy in public and crime scene DNA before genetic sequencing technology becomes affordable and widely used.¹⁸²

The information that should be protected from a warrantless search should be the same information that a court would recognize as infringing an individual's right to privacy.¹⁸³ The privacy rights of an individual depend on the standard set forth in Justice Harlan's concurring opinion in the U.S. Supreme Court's 1967 decision in *Katz v. United States*, which states that an individual must have a subjective expectation of privacy and society must recognize that this expectation is reasonable for a search to violate the Fourth Amendment.¹⁸⁴ Currently, individuals likely have a subjective expectation that skin and hair left behind in open spaces is not being used to uncover every genetic disposition they have toward diseases, certain behaviors, and so forth.¹⁸⁵ In addition, society recognizes that this expectation is reasonable, as the strong legal protection for confidential medical records amply demonstrates.¹⁸⁶ As a result, although it seems clear that uncovering one's entire genome infringes an individual's privacy rights, the question remains as to how much information can be uncovered to satisfy law enforcement's interests without infringing on the individual's right to privacy.¹⁸⁷

B. *Informational Privacy Should Protect Non-Visible Genetic Traits*

The information that can be uncovered from an individual's genome should be split into two groups: phenotypic information and non-

¹⁸⁰ See KRIMSKY & SIMONCELLI, *supra* note 1, at 99.

¹⁸¹ See *id.*; Rothstein & Talbott, *supra* note 80, at 162; Suter, *supra* note 60, at 398–99.

¹⁸² See KRIMSKY & SIMONCELLI, *supra* note 1, at 99; Rothstein & Talbott, *supra* note 80, at 162; Suter, *supra* note 60, at 398–99.

¹⁸³ See KRIMSKY & SIMONCELLI, *supra* note 1, at 99.

¹⁸⁴ See 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

¹⁸⁵ See *State v. Athan*, 158 P.3d 27, 51–53 (Wash. 2007) (Fairhurst, J., dissenting); Suter, *supra* note 60, at 356–58.

¹⁸⁶ See *Athan*, 158 P.3d 27, 51–53; Suter, *supra* note 60, at 356–58.

¹⁸⁷ See *Athan*, 158 P.3d 27, 51–53; Suter, *supra* note 60, at 356–58.

phenotypic information.¹⁸⁸ Phenotypic information contains information about a person's physical appearance.¹⁸⁹ Phenotypic testing could use DNA to uncover what a potential perpetrator may look like.¹⁹⁰ Non-phenotypic information is everything else on an individual's genome, such as predisposition to diseases or certain behavioral traits.¹⁹¹

1. Phenotypic Information

Determining phenotypic information from routinely shed DNA found at a crime scene should not have any implications on an individual's right to privacy.¹⁹² Because phenotypic information merely describes the way that individuals look, such information cannot be considered private.¹⁹³

First, by venturing out in public, an individual exposes his or her phenotypic information, such as hair color, eye color, and so forth, to the world.¹⁹⁴ As stated in *Katz*, what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.¹⁹⁵ Despite the fact that *Katz* recognized that what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected, phenotypic information is the type of information that is almost impossible to keep private.¹⁹⁶ Although disguises, such as hair dyes and contact lenses, can change one's physical appearance, these alternatives do not change the fact that an individual knowingly risks exposure of his or her phenotypic information, whether it be from a contact lens falling out, a visible surgery scar, or a brown hair peeking through a full head of blond hair.¹⁹⁷ Whether a witness to a crime relays information about a potential suspect or the police uncover that information via discarded DNA, an in-

¹⁸⁸ See KRIMSKY & SIMONCELLI, *supra* note 1, at 90; Koops & Schellekens, *supra* note 69, at 164–65.

¹⁸⁹ See KRIMSKY & SIMONCELLI, *supra* note 1, at 90; Koops & Schellekens, *supra* note 69, at 164–65.

¹⁹⁰ See KRIMSKY & SIMONCELLI, *supra* note 1, at 90; Koops & Schellekens, *supra* note 69, at 164–65.

¹⁹¹ See KRIMSKY & SIMONCELLI, *supra* note 1, at 90; Koops & Schellekens, *supra* note 69, at 164–65.

¹⁹² See *infra* notes 194–201 and accompanying text.

¹⁹³ See *infra* notes 194–201 and accompanying text.

¹⁹⁴ See *Katz*, 389 U.S. at 351–52.

¹⁹⁵ *Id.*

¹⁹⁶ See Koops & Schellekens, *supra* note 69, at 164–65.

¹⁹⁷ See *id.* at 182.

dividual has exposed this information to the public, extinguishing any privacy right.¹⁹⁸

Second, although one could argue that routinely shed DNA should not qualify as knowing exposure of personal information to the public, an individual does not have an expectation of privacy in his or her own phenotypic information that society would recognize as reasonable.¹⁹⁹ The *Katz* test requires that an individual have a subjective expectation of privacy and that society recognize that this expectation is reasonable.²⁰⁰ By venturing into public, an individual is unable to retain the anonymity that he or she might enjoy in private, and, as a result, society would not recognize this expectation of anonymity to be reasonable, especially if one is a suspect or potential witness to a crime.²⁰¹

2. Non-Phenotypic Information

Non-phenotypic information includes information such as disposition toward certain diseases or behavioral tendencies, and this information should be protected from warrantless search.²⁰² Non-phenotypic information is identical to highly private and sensitive medical facts, in which individuals have the highest expectation of privacy.²⁰³ As the U.S. Court of Appeals for the Ninth Circuit recognized in 1998 in *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, privacy rights can be circumvented if the testing is authorized, or if individuals reasonably should have known that DNA samples would be used for certain kinds of testing and failed to object.²⁰⁴

In the case of non-phenotypic information found at crime scenes, it is important to recognize that, unlike the holding in 2007 in *State v. Athan*, some privacy rights do exist in discarded genetic material.²⁰⁵ In 2001 in *Kyllo v. United States*, the U.S. Supreme Court recognized that the use of technology not in general public use to obtain information

¹⁹⁸ See *Katz*, 389 U.S. at 351; Koops & Schellekens, *supra* note 69, at 182.

¹⁹⁹ See *Katz*, 389 U.S. at 361 (Harlan, J., concurring); see also *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (implying that an individual does not have a reasonable expectation of privacy in information that cannot be obtained without a physical intrusion into a constitutionally protected area).

²⁰⁰ 389 U.S. at 361 (Harlan, J., concurring).

²⁰¹ See *id.*

²⁰² See Koops & Schellekens, *supra* note 69, at 182–83.

²⁰³ See *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269–70 (9th Cir. 1998).

²⁰⁴ See *id.* at 1270.

²⁰⁵ See *infra* notes 206–210 and accompanying text.

that could not otherwise have been obtained without “physical intrusion into a constitutionally protected area” violates the reasonable expectation of privacy protected by the Fourth Amendment.²⁰⁶ Until people can readily sequence genomes in a way that constitutes general public use, this test should control whether or not the sequencing of a genome without permission violates an individual’s privacy.²⁰⁷ Apart from the testing of routinely shed DNA, this detailed medical information in a person’s non-phenotypic information can only be obtained through a mandatory intrusion into a person’s body from a DNA test, unlike phenotypic information which can be obtained through eyewitness testimony by a casual observer without intruding on a constitutionally protected area.²⁰⁸ Courts have held that these kinds of warrantless intrusions are only permissible when an important governmental interest outweighs the individual’s privacy interest and the individual has not authorized these intrusions.²⁰⁹ With respect to non-phenotypic information, the individual’s privacy interest is so strong that there is unlikely to be a governmental interest that can outweigh the privacy interest, and thus, like the private data in medical records, the government should be required to seek a warrant and to defend its intrusion into an individual’s privacy.²¹⁰

C. Discarded DNA Is Not Abandoned

Although the court in *Athan* held that there is no expectation of privacy in discarded genetic material because it is abandoned, the concurring opinion cautioned that this dicta should be limited in future application.²¹¹ Abandonment in the search and seizure context is not the same as abandonment in property law.²¹² In the Fourth Amend-

²⁰⁶ 533 U.S. at 40.

²⁰⁷ See Suter, *supra* note 60, at 357–58. Even if sequencing technology becomes publicly available, the reasonable expectation that routinely shed DNA will not be sequenced should prevent such sequencing from gaining acceptance. See *Kyllo*, 533 U.S. at 40; *Norman-Bloodsaw*, 135 F.3d at 1270.

²⁰⁸ See *Kyllo*, 533 U.S. at 40.

²⁰⁹ See *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 603, 622 (1989); *Schmerber v. California*, 384 U.S. 757, 767 (1966); *Norman-Bloodsaw*, 135 F.3d at 1270.

²¹⁰ See KRIMSKY & SIMONCELLI, *supra* note 1, at 100–01. Although the government may have an interest in obtaining this information, this interest must outweigh the highest expectation of privacy an individual has in keeping this information private, and this kind of calculation is the type that an impartial magistrate should make in issuing a warrant. See *Skinner*, 489 U.S. at 622; KRIMSKY & SIMONCELLI, *supra* note 1, at 100–01.

²¹¹ 158 P.3d at 44 n.1 (Alexander, C.J., concurring).

²¹² See *State v. Daniels*, 576 So. 2d 819, 823 (Fla. Dist. Ct. App. 1991); *State v. Kerr*, 470 A.2d 670, 676 (Vt. 1983); 79 C.J.S. *Searches* § 38 (2012).

ment context, abandonment occurs only if a person relinquishes a reasonable expectation of privacy in an item, for example by leaving an item unsecured in a public place.²¹³ Another requirement is that abandonment must be voluntary.²¹⁴ Although venturing into public is a voluntary act, shedding DNA is involuntary.²¹⁵ Thus, even though leaving a piece of tangible property behind in a public place is considered abandonment, the inevitable and uncontrollable shedding of skin cells and other genetic material is fundamentally different because shedding is not a conscious, voluntary act.²¹⁶ Because DNA found in a public space such as a crime scene was likely left behind unintentionally by routine shedding, the genetic material has not been abandoned or relinquished and, as a result, an individual's privacy right in the private, non-phenotypic information contained in that DNA should continue to be protected.²¹⁷

Although routinely shed DNA is uncontrollable and thus should not be considered abandoned, this rule could be reconciled with case law by requiring some conscious or subconscious act for DNA to be considered abandoned.²¹⁸ The *Athan* court stated that saliva from an envelope was abandoned,²¹⁹ and other courts have similarly found that saliva from cigarettes²²⁰ and cups was abandoned.²²¹ This abandonment of genetic material, although subconscious and arguably unintentional, is fundamentally different from routinely shed DNA because the act that caused the DNA to be left behind was voluntary.²²² In these cases, individuals can control the relinquishment of genetic material, they just elect not to or ignore such a right.²²³ This volitional aspect is

²¹³ See *United States v. Stevenson*, 396 F.3d 538, 546 (4th Cir. 2005); *State v. Rynhart*, 125 P.3d 938, 943 (Utah 2005); 79 C.J.S. *Searches* § 38.

²¹⁴ See *United States v. Morgan*, 936 F.2d 1561, 1570 (10th Cir. 1991); 79 C.J.S. *Searches* § 38.

²¹⁵ See *Athan*, 158 P.3d at 44 n.1 (Alexander, C.J., concurring).

²¹⁶ See *id.*; see also *Suter*, *supra* note 60, at 353–58 (arguing that routinely shed DNA is not relinquished or abandoned because such shedding is involuntary and there is no reasonable expectation that this genetic information will be analyzed; thus, privacy rights have not been extinguished in routinely shed DNA).

²¹⁷ See *Rothstein & Talbott*, *supra* note 80, at 156.

²¹⁸ See *Williamson v. State*, 993 A.2d 626, 634–35 (Md. 2010); *Commonwealth v. Perkins*, 883 N.E.2d 230, 239 (Mass. 2008); *Athan*, 158 P.3d at 37.

²¹⁹ 158 P.3d at 37.

²²⁰ *Perkins*, 883 N.E.2d at 239.

²²¹ *Williamson*, 993 A.2d at 634–35.

²²² See *id.*; *Perkins*, 883 N.E.2d at 239; *Athan*, 158 P.3d at 37.

²²³ See *Williamson*, 993 A.2d at 634–35; *Perkins*, 883 N.E.2d at 239; *Athan*, 158 P.3d at 37.

markedly absent when an individual routinely sheds DNA.²²⁴ As a result, unlike the volitional aspect of leaving behind saliva on a cigarette or a cup, the fact that an individual decided to venture out into public should not destroy any protectable privacy right in routinely shed genetic material because an individual has no reasonable expectation that their shed DNA could possibly be analyzed.²²⁵

Although some cases state that any genetic material left behind as a result of a volitional act is abandoned, this is not necessary.²²⁶ Genetic material that is left behind as a result of a volitional act is often subconscious, and the distinction between subconscious and involuntary is only semantic.²²⁷ A person who licks an envelope closed should not receive less protection from the disclosure of his or her medical history than a person who sheds skin cells on that envelope, because regardless of how the DNA gets on the envelope, there is no difference in the privacy expectations of these two individuals.²²⁸ As a result, the *Athan* dissent's reasoning that there is a privacy interest in discarded DNA should prevail.²²⁹ Therefore, instead of barring the use of routinely shed DNA entirely, law enforcement should be permitted to analyze discarded DNA for identification purposes, namely phenotypic data.²³⁰

D. *Police Should Obtain a Warrant to Uncover Non-Phenotypic Data from Routinely Shed DNA*

There is no privacy interest in phenotypic data contained in discarded DNA.²³¹ As a result, when routinely shed DNA is found at a crime scene, there is no reason that the phenotypic information cannot be extracted to help narrow lists of suspects or serve other law enforcement purposes.²³² When it comes to non-phenotypic information, however, it seems clear that a privacy interest exists.²³³ Indeed, police

²²⁴ See *Williamson*, 998 A.2d at 634–35; *Perkins*, 883 N.E.2d at 239; *Athan*, 158 P.3d at 37; Suter, *supra* note 60, at 352–58.

²²⁵ See *Williamson*, 998 A.2d at 634–35; *Perkins*, 883 N.E.2d at 239; *Athan*, 158 P.3d at 37; Suter, *supra* note 60, at 352–58.

²²⁶ See *supra* notes 218–225 and accompanying text.

²²⁷ See Daniel Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1530–31 (2010) (arguing that this semantic test makes the current Fourth Amendment jurisprudence impracticable in the future); see also *infra* notes 222–225 and accompanying text.

²²⁸ See *Athan*, 158 P.3d at 41–42 (Fairhurst, J., dissenting).

²²⁹ See *id.*

²³⁰ See *supra* notes 180–229 and accompanying text.

²³¹ See *supra* notes 180–201 and accompanying text.

²³² See *Koops & Schellekens*, *supra* note 69 at 182–83.

²³³ See *supra* notes 202–210 and accompanying text.

currently need a warrant to access medical records that may contain this private information.²³⁴ The warrant process could also serve as a buffer between law enforcement and the private information contained in routinely shed DNA.²³⁵ Therefore, the government should be required to obtain a warrant and to articulate an interest that outweighs an individual's right to privacy in non-phenotypic information.²³⁶

As for decoding areas of the genome that code for both phenotypic and non-phenotypic information absent a warrant, such as an area that codes for both gender and predisposition for a disease, this information should only be uncovered to the extent that it reveals phenotypic information.²³⁷ The Supreme Court has recognized that searches conducted without warrants have been held unlawful notwithstanding facts unquestionably showing probable cause because the Constitution requires deliberate, impartial judgment of a judicial officer to be interposed between a citizen and the police.²³⁸ Although in these instances some phenotypic information may provide glimpses into private non-phenotypic information, these observations could be uncovered by an observer's naked eye and knowledge of these correlations.²³⁹ Thus, associations between phenotypic and non-phenotypic information in these situations should not prevent phenotypic information from being uncovered solely for identification purposes.²⁴⁰

²³⁴ See KRIMSKY & SIMONCELLI, *supra* note 1, at 100–01.

²³⁵ *See id.*

²³⁶ *See id.*

²³⁷ See Rothstein & Talbott, *supra* note 80, at 160–61. Extracting phenotypic information from those whose DNA is already in CODIS and including it in the CODIS database without including any non-phenotypic information from that same region of an individual's genome would likely not violate any expectation of privacy that society is willing to recognize as reasonable because the only information that is being stored and potentially disseminated is phenotypic information, which an individual cannot reasonably expect to keep private. *See id.*

²³⁸ *Katz*, 389 U.S. at 357.

²³⁹ *See infra* note 240. Although some studies show correlations between trivial traits and sensitive information (i.e., that left-handed people appear to die more often in an accident than right-handed people), there is no reason that uncovering this information through genetic testing would infringe on an individual's privacy any more than the normal observation of a witness. *See* Koops & Schellekens, *supra* note 69, at 182 n.90. In addition, unlike the arguments of scholars like Rothstein and Talbott, filtering phenotypic information out from non-phenotypic information should not be any more difficult in practice than filtering out the thirteen loci used in DNA fingerprinting from all of the potential material in a genome. *See* Rothstein & Talbott, *supra* note 80, at 160–61.

²⁴⁰ *See* Koops & Schellekens, *supra* note 69, at 182 n.90.

E. State Databases Should Not Retain DNA Samples Indefinitely

DNA databases should not contain physical DNA samples and, to the extent that they do, the DNA samples should not be retained indefinitely.²⁴¹ Two main justifications have been presented for maintaining and using DNA databases: deterring future crime and preventing recidivism by facilitating the identification of repeat offenders.²⁴² Because both of these purposes can be achieved using only phenotypic information logged in DNA databases, there is not a sufficient reason for states to retain the actual DNA samples in perpetuity.²⁴³

Permanent retention of DNA samples should not be permitted for four main reasons.²⁴⁴ First, despite the fact that some courts have ruled that convicted felons have a reduced right of privacy, maintaining DNA samples and having potential access to non-phenotypic information is not required for the government to accomplish its goals of combating recidivism and deterring future crime.²⁴⁵ These goals can be accomplished simply with the inclusion of phenotypic information in a DNA database.²⁴⁶ Second, because phenotypic information extracted from DNA is easily confirmed by visual observation, the justification that the samples must be maintained in case mistakes are made would no longer apply.²⁴⁷ Third, because DNA samples are allowed to be taken from arrestees, the retention of samples from those who are acquitted is unreasonable as these individuals do not have a diminished privacy right.²⁴⁸ This means that the privacy rights for those who are acquitted vastly outweigh the almost negligible governmental interests in maintaining this genetic information.²⁴⁹ Finally, the last justification for law enforcement officials retaining these samples is so that, as new technology arises, the samples can be used to update the databases to new standards.²⁵⁰ Once the genome is understood and phenotypic information is distinguishable from non-phenotypic information, the databases will already contain all the required phenotypic information, and there would be no justification at that point for having private, non-

²⁴¹ See Suter, *supra* note 60, at 339–42.

²⁴² Etzioni, *supra* note 3, at 200–01.

²⁴³ See *id.*; Suter, *supra* note 60, at 339–42.

²⁴⁴ See *infra* notes 245–251 and accompanying text.

²⁴⁵ See Suter, *supra* note 60, at 339–42; *supra* notes 145–163 and accompanying text.

²⁴⁶ See Suter, *supra* note 60, at 339–42; *supra* notes 145–163 and accompanying text.

²⁴⁷ See Koops & Schellekens, *supra* note 69, at 183.

²⁴⁸ See Suter, *supra* note 60, at 339–42; *supra* note 147 and accompanying text (explaining that courts afford less privacy protection to prisoners).

²⁴⁹ See *id.*

²⁵⁰ NAT'L INST. OF JUSTICE, *supra* note 161.

phenotypic information readily accessible in these genetic databases, which means that policies must be implemented so that samples are not retained indefinitely.²⁵¹

Because genome sequencing may become more popular in the future, states should provide some sort of legal check to prevent DNA databases from potentially including private non-phenotypic information.²⁵² Without providing for the destruction of DNA samples, there is a legitimate fear that these databases may take on new functions that invade the privacy rights of individuals.²⁵³ Although police can and should use fingerprints, which do not say anything about a person's health, propensity for a particular disease, race or gender characteristics, or propensity for certain conduct, law enforcement personnel should not be trusted to protect individuals' genetic privacy interests without any legal or legislative oversight.²⁵⁴

CONCLUSION

Genetic information from routinely shed DNA can be broken up into two types, phenotypic and non-phenotypic information. Because phenotypic information describes visible information about an individual that can be uncovered easily without sequencing the DNA, an individual does not have a significant privacy interest in this kind of information. As a result, there are no privacy implications when crime scene DNA is sequenced to narrow a list of suspects.

Non-phenotypic information, on the other hand, contains private information. As a result, an individual has a reasonable expectation that this information will be kept private and will not be unreasonably uncovered. Despite arguments that the privacy interest in this kind of information is extinguished because crime scene DNA has been "abandoned" or "relinquished," such arguments should not be applied to circumvent the warrant process. Instead, just as in cases of medical records, the government should have to show probable cause or some sort of individualized suspicion in order to uncover this kind of information. Otherwise, innocent individuals may soon find their entire ge-

²⁵¹ See *id.*

²⁵² See Rothstein & Talbott, *supra* note 80, at 158; see also WISC. STAT. ANN. § 165.77 (West 2009) (requiring destruction after analysis has been completed and the applicable court proceedings have ended). Reportedly, no samples have yet been destroyed. Rothstein & Talbott, *supra* note 80, at 158.

²⁵³ See Simoncelli & Steinhardt, *supra* note 61, at 203.

²⁵⁴ See Rothstein & Talbott, *supra* note 80, at 158; *supra* notes 62–92 and accompanying text.

nomes in DNA databases not because they have committed any crime, but instead because they ventured into public and unknowingly lost some hair or skin particles.

Finally, because physical DNA samples contain both phenotypic and non-phenotypic information, states should not retain physical DNA samples in perpetuity. The purpose of DNA databases is to prevent future crime and to combat recidivism by using the information to catch repeat offenders. The government's purpose in maintaining DNA samples does not outweigh the privacy rights of individuals because maintaining these samples ostensibly serves no governmental purpose. Despite the fact that many courts have found that convicted felons have a reduced privacy interest due to their past crimes, this privacy interest is diminished, not non-existent. In addition, because innocent people may be included in this database, their right to privacy in their genetic information should outweigh the minimal governmental interest in having access to non-phenotypic information. As a result, states should adopt some sort of limits on the duration of retention of physical DNA samples.

DAVID GUSELLA