



DNA and Its Privacy

Citation

Coodly, Lavanya R. 2019. DNA and Its Privacy. Master's thesis, Harvard Extension School.

Permanent link

<http://nrs.harvard.edu/urn-3:HUL.InstRepos:42006723>

Terms of Use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA>

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. [Submit a story](#).

[Accessibility](#)

DNA and Its Privacy

Lavanya Coodly

A Thesis in the Field of Legal Studies
for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

November 2019

Abstract

[W]e can't go anywhere without leaving a bread-crumbs trail of identifying DNA matter. If we have no legitimate expectation of privacy in such bodily material, what possible impediment can there be to having the government collect what we leave behind, extract its DNA signature and enhance CODIS to include everyone?

—Judge Alex Kozinski, dissenting in *United States v. Kincaid*

When you've licked a stamp on your tax return you've sent the government a DNA sample. . . .

—Victor Weedn, Head of Armed Forces DNA Identification Laboratory

When we visit a doctor's office and leave samples of blood or urine, sip a drink out of a glass in a restaurant, comb our hair, or visit a salon or a spa, it turns out that we are inadvertently leaving behind traces of our DNA. Almost every place we go, our genetic identity is discarded, even if it is in trace amount. Should the medical laboratory, restaurant, spa, or salon be permitted to collect the DNA left behind, store it indefinitely, and share or transfer our genetic material to another location without regulation? Why should we care about care about DNA ownership? This matters to us because DNA is a blueprint of who we are, differentiating each of us from the other. At the same time, DNA is inherited and can reveal blood relatives and extremely personal information that could potentially disclose details about us that we may not want others to find out. Susceptibility to genetic disease, color of hair and eyes, and even personal choices stand to become unraveled in our DNA code as scientific research continues to identify genes and functions.

Loss of ownership to our genetic information can occur in one of two major ways. First, DNA might be shed unintentionally. Second, DNA might be submitted voluntarily.

In both cases, we lose legal ownership to our genetic information (DNA). As it stands today, it also turns out that our DNA is no longer our private property because, once unintentionally discarded or voluntarily submitted, we have potentially relinquished our rights to its exclusive proprietorship. One of the purported reasons for the lack of ownership status is that once left behind in a public space, DNA is considered discarded or abandoned and existing Fourth Amendment law does not seem to apply. Therefore, once it is considered abandoned, DNA has the potential of becoming public property, where the finder is the keeper who will ultimately have control over its use.

Advances in technologies have compounded the ways in which individual identities are evolving: genetic (DNA), informational (public records), and digital (cyberspace) identities are but a few examples. The time may now have come when the traditional U.S. Fourth Amendment analysis is no longer suited in the world in which we live, a world in which the body itself may become a rather archaic way of defining the individual.

This thesis contends that our DNA should not be considered abandoned when we discard it in our hair, skin, drinking cup, or cigarette butt. It argues that neither should DNA be considered “public” when we voluntarily give blood or urine to a doctor or employer for analysis while complying with existing rules and regulations, and the same holds true when we donate blood or organs to benefit society. This thesis supports placing legislation granting ownership and sole proprietorship of bodily fluids and along with it the cells and DNA contained within to the donor, whose permission must be sought before duplicating, testing, sharing, donating, or analyzing. Under this author’s

view, failure to do so would be considered an infringement on the property rights of that individual, an offense that is punishable by law.

Dedication

I dedicate this effort to my parents, who would have been delighted for me to reach this milestone. I also dedicate this work to my husband and son, who have been constantly supportive of my desire to seek an education at the very best institution and understanding through every step of the journey.

Acknowledgments

I am grateful to Harvard University for the opportunity to learn and grow intellectually. I wish to express my gratitude to Dr. Ostrowski for patiently guiding me through the process of writing. I am immensely grateful to Dr. Frederick Bieber for directing the work, leading useful discussions, and mentoring with generosity.

Table of Contents

Dedication.....	vi
Acknowledgments.....	vii
Introduction.....	1
Chapter I. Background.....	5
Forensic DNA Analysis Technology.....	8
DNA Genealogy, Technology, and Background.....	10
Debate on Public Databases.....	12
Use of DNA in Law Enforcement.....	26
Chapter II. Fourth Amendment Jurisprudence.....	28
Scholarly Conclusions and Case Law.....	29
People v. Sigsbee.....	35
Commonwealth v. Bly.....	37
State v. Reed.....	39
Commonwealth v. Cabral.....	41
State vs. Christian.....	42
State v. Athan.....	45
Maryland v. King.....	47
Carpenter v. United States.....	50
R. v. Stillman.....	57
Collins-Stillman Analysis.....	60

Expectations of Privacy	62
Solving Cold Cases through STR Analysis	64
Tracking Down BTK	66
Popular DJ Caught after 26 Years	68
Reasonable Expectations of Privacy in Discarded Items.....	71
Historical Views on Property and Place	80
Katz v. United States.....	80
Kyllo v. United States	84
United States v. Jones	85
Surreptitious DNA Harvesting and Privacy.....	87
Physical Boundaries.....	92
Skinner v. Railway Labor Executives Association.....	93
National Treasury Employees Union v. Von Raab.....	96
Out of Body DNA Collection	97
Science and Technology	99
Understanding Privacy.....	102
The Road to Genetic Privacy	103
Chapter III. Reasonableness of Expectations of Genetic Privacy.....	113
Genetic Database Opinions.....	114
The Protected Core: A Kaleidoscope of Identity	121
Physical Privacy.....	123
Analogous Case Law	126
Analogous Scientific Testing.....	128

Analogous Fingerprints.....	129
Informational Privacy	132
Predictive Information	133
Shared Information	136
Personal and Intimate Information.....	141
Powerful Information.....	141
Dignitary Privacy	146
Societal Perspectives on Genetic Privacy	154
Print Media.....	156
Chapter IV. Discussion and Conclusion	159
Discussion	159
Conclusion	173
Appendix 1. Survey Results.....	178
References.....	184

Introduction

Genetic privacy and rights to our most personal information have recently become topics of hot debate in the criminal justice system. Advances in genealogical studies and the subsequent success of using DNA as evidence to crack cold cases¹ have brought tremendous attention to this area of study. Societal interest and curiosity about genealogy, including the hope of finding long lost relatives² or to understand and come to terms with one's own ethnic background, have brought about hugely successful, large scale, for-profit enterprises like Ancestry.com, 23andme.com, and myheritage.com, to name a few. Law enforcement practices in DNA collection have also come under close scrutiny as officials also collect DNA and subject it to forensic analysis to identify elusive criminals and solve cold cases.³

To date, DNA harvesting by genealogy companies and the police force is unregulated by the U.S. Fourth Amendment.⁴ DNA can be extracted from discarded

¹ One of the earliest uses of this technique is attributed to Boston detectives, who in 1996 collected DNA from a suspect by offering him a cigarette. See Willing, "Police Dupe Suspects," A3. See also Gillespie, "Need for Greed Ends," A20, which reports that police around the country have "put suspects under surveillance in hopes that they might discard a cigarette or wad of gum from which DNA could be drawn." van Derbeken, "How Alleged Serial Killer," A1.

² Harmon, "'Stalking Strangers' DNA to Fill," A1.

³ Curley and Caperna, "The Brave New World," 22, 27 (noting that with regard to "abandoned DNA" ... "the law may need to address previously unthought of privacy concerns").

⁴ See, for example, Harmon, "Lawyers Fight DNA Samples," A1, which describes differing opinions on the legality of surreptitiously collected DNA samples. Existing discussions of abandoned DNA are largely brief citations of it as a phenomenon to watch. See, for example, Curley and Caperna, "The Brave New World," 22, 27 with regard to "abandoned DNA," "the law may need to address previously unthought of privacy concerns". The most extensive discussion of the issue thus far has been presented by Ed Imwinkelried and D. H. Kaye, "DNA Typing: Emerging," 436-440, who identify "abandoned DNA" as one of many "emerging or neglected" issues in legal analysis of DNA sampling: "Courts may find it a

cigarette butts,⁵ saliva,⁶ blood,⁷ semen,⁸ urine,⁹ drinking cups,¹⁰ licked envelopes,¹¹ and expectorant¹² of any individual, including suspected criminals. Subsequently, this “discarded” DNA can be tested clandestinely as part of an investigation and may be introduced in court as evidence to demonstrate guilt¹³ or to exclude a suspect or demonstrate innocence of putative suspects or those incorrectly convicted.¹⁴

While bringing criminals to justice and closure to families of victims are positive outcomes to society,¹⁵ other unintended consequences of forensic DNA analysis by law enforcement and private genealogy firms could theoretically exist. The person who volunteers a DNA sample while signing a consent form could nevertheless be unaware of other potential uses of his or her genetic information.¹⁶ Similarly, consumers of

small step to conclude the warrantless collection of inadvertently abandoned DNA does not violate the Fourth Amendment,” at 439.

⁵ Hochmeister et al., “PCR-Based Typing,” 229.

⁶ Sweet and Shutler, “Analysis of Salivary DNA,” 1069.

⁷ Budowle et al., “Simple Protocols for Typing,” 1559-1560.

⁸ Budowle et al., “Simple Protocols for Typing,” 1559-1560.

⁹ Yasuda et al., “A Simple Method of DNA Extraction,” 108.

¹⁰ van Derbeken, “How Alleged Serial Killer,” A1.

¹¹ Ho, “Man is Sentenced in ’82,” B1; Johnson, “N.J. Man Convicted,” B1; Nelkin and Andrews, “DNA Identification and Surveillance Creep,” 689, 693.

¹² Francescani, “Sex Fiend Admits He Killed,” 11 (reporting on defendant linked to five murders after police collected saliva on the ground outside of police station, and after defendant refused to provide DNA sample).

¹³ Nakashima, “From DNA of Family,” A01.

¹⁴ See generally Innocence Project, last updated 2019, <https://www.innocenceproject.org/>

¹⁵ Nakashima, “From DNA of Family,” A01.

¹⁶ See, for example, Grand, “The Bleeding of America,” 2280, noting that law enforcement agencies may be creating massive database of DNA profiles; Willing, “Local DNA Labs Avoid,” A1,

genealogy searches who voluntarily submit their blood or saliva with the hope of finding long lost loved ones or analyze their ancestry would be oblivious of other ways for-profit companies might utilize their findings by selling the data to pharmaceutical companies.¹⁷ In both scenarios, asymmetric information and moral hazard could prevail.

Asymmetric information refers to unequal information from a consumer's perspective.¹⁸ A for-profit genealogy company may not fully disclose its true intention with a subscriber's or customer's genetic information. Alternatively, once the genealogy company has received a payment and DNA sample from a customer, the company may decide to sell the customer's genetic information to another party unbeknownst to the consumer.¹⁹ The basis for this type of emboldened disregard for consumer privacy may stem out of two reasons: the consumer is unaware that his or her personal information carries value, and monitoring or litigation and costs are costly and time consuming. The time, expense, and inconvenience of tracking a company's policies and management decisions are beyond the scope of most ordinary consumers. For this reason, a consumer's loss of privacy can be attributed to moral hazard by the genealogy company who could potentially engage in unethical conduct and not pay a price.

noting that "a growing number of police crime labs are adding DNA from suspects to databases"; Greenhouse, "Law Seeks to Ban," at <https://www.nytimes.com/2009/11/16/business/16genes.html>, explaining "employers or health insurers would discriminate against them, perhaps by firing them or denying coverage."

¹⁷ Ducharme, "A Major Drug Company," at <https://time.com/5349896/23andme-glaxo-smith-kline/>. GSK, "GSK and 23andMe Sign," at <https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines/>.

¹⁸ Agarwal, "Asymmetric Information," at <https://www.intelligenteconomist.com/asymmetric-information/>.

¹⁹ Herper, "23andMe Gets \$300 Million," at <https://www.forbes.com/sites/matthewherper/2018/07/25/23andme-gets-300-million-boost-from-glaxo-to-develop-new-drugs/#33db82743213>; Geggel, "23andMe Is Sharing," at <https://www.livescience.com/63173-23andme-partnership-glaxosmithkline.html>.

It seems that these days, even amateur genealogists have access to DNA and can obtain it without the knowledge and consent of the DNA owner. During a well-known celebrity divorce, a private investigator obtained DNA surreptitiously by isolating it from dental floss discarded in the garbage by the husband and subsequently used the information as evidence in a paternity analysis to benefit the client.²⁰

Under present interpretation of the Fourth Amendment and laws regarding clandestine DNA harvesting, individuals are not protected from asymmetry of information regarding DNA analysis or informed of its potential misuse further downstream. This thesis examines landmark cases in which the Fourth Amendment protects current societal understanding of a reasonable expectation of privacy and discusses how it must now expand from tangible ownership of property, house, and home to include genetic privacy.

²⁰ Halbfinger and Weiner, “Celebrity Lawyers in Talks,” B7.

Chapter I.

Background

Comparing fingerprints and blood samples left behind in a crime scene with those taken from an alleged suspect are traditionally acceptable methods of identifying perpetrators and differentiating them from victims of a crime. By providing a suspect's fingerprints as evidence in a court of law, such evidence may assist the court system, which could ultimately convict or exonerate suspects.²¹ More recently, law enforcement officials and forensic investigators have acquired increasingly sensitive tools to aid in the identification of individuals of interest. These tools may help convict or acquit suspects.

Advances in DNA technology and the availability of extra-corporeal DNA in crime scenes have made forensic analyses possible and expanded investigative options for the police and other law enforcement officials.²² The same technological breakthroughs have also facilitated kinship and genealogy searches and led to convictions years—or even decades—later in hundreds of cold cases. DNA obtained from relatives of elusive serial criminals has led to their capture several decades after their killing sprees, brought them to justice, and provided closure to families of victims.²³ DNA analysis has also led to the exoneration of hundreds of wrongfully convicted persons, some of whom

²¹ National Research Council, *DNA Technology in Forensic Science*, 28.

²⁶ Willing, "Police Dupe Suspects," A3.

²³ Bieber et al., "Finding Criminals through DNA," 1315; Paoletti et al., "Assessing the Implications," 161; Nakashima, "From DNA of Family," A01.

have served more than twenty years in prison for crimes for which they were convicted but that they did not commit.²⁴

In the past, before the late 1980s, tools for investigative techniques were fewer and the police did not have the analytical technology that is available today for isolating and studying DNA in a way that could individualize identification. After U.S. commercial laboratories began utilizing forensic DNA for investigative purposes,²⁵ the FBI adopted DNA analysis in their casework in 1988.²⁶ Today, the United States has over 150 public laboratories dedicated to forensic DNA analysis.²⁷

Before 1988, comparisons of latent digital fingerprints, other impression evidence, and ABO blood typing were the main sources of forensic evidence used to connect a suspect to an object or to a crime scene.²⁸ However, these techniques have their limitations.²⁹ For example, fingerprints require the suspect to have handled at least one item with bare fingers, and the same ABO blood type can be shared by many.³⁰ Therefore, traditional fingerprint analysis and ABO blood typing cannot necessarily rule out the involvement of other perpetrators in a crime investigation. The development of forensic DNA analysis has greatly enhanced the ability of investigators to identify

²⁴ See generally Innocence Project, last updated 2019, <https://www.innocenceproject.org/>.

²⁵ National Research Council, “DNA Technology in Forensic Science,” 28.

²⁶ National Research Council, “DNA Technology in Forensic Science,” 28.

²⁷ Butler, *Forensic DNA Typing*, 3.

²⁸ National Research Council, “DNA Technology in Forensic Science,” *supra* note 7, 27–29.

²⁹ Butler, *Forensic DNA Typing*, 3.

³⁰ Butler, *Forensic DNA Typing*, *supra* note 21, 5.

criminal suspects due to its increased specificity and sensitivity and the exacting nature of the analysis.³¹

DNA can be inadvertently shed by a suspect or victim, facilitating its availability in multiple sources. DNA exists in every nucleated cell in the human body in blood,³² semen,³³ hair,³⁴ fingernails,³⁵ and muscle tissue.³⁶ DNA can be also found in bodily waste such as saliva,³⁷ urine,³⁸ feces,³⁹ and dandruff.⁴⁰ It is also left behind on cigarette butts,⁴¹

³¹ See Bieber, "Science and Technology of Forensic DNA Profiling: Current Use and Future Predictions," in *DNA and the Criminal Justice System: The Technology of Justice*, ed. David Lazer (discussing techniques of the forensic analysis of DNA and provides a basis for its understanding).

³² Budowle et al., "Simple Protocols for Typing," 1559-1560.

³³ Budowle et al., 1559-1560.

³⁴ Higuchi et al., "DNA Typing from Single Hairs," 543; Wilson et al., "Extraction, PCR Amplification and Sequencing," 662.

³⁵ DNA is contained in blood, semen, skin cells, tissue, organs, muscle, brain cells, bone, teeth, hair, saliva, mucus, perspiration, fingernails, urine, and feces. See National Commission on the Future of DNA Evidence, U.S. Department of Justice, *What Every Law Enforcement*, 2 (noting that only a few cells can be sufficient to obtain useful DNA information); see also Ross, "A Trail of Genetic Evidence," *supra* note 3 (reporting that 500 picograms to one nanogram is sufficient for a good DNA sample). Wiegand et al., "DNA Typing of Debris," 81.

³⁶ Hochmeister et al., "PCR-Based Typing," 19.

³⁷ See Sweet and Shutler, "Analysis of Salivary DNA," *supra* note 7.

³⁸ See Yasuda et al., "A Simple Method of DNA Extraction," *supra* note 10.

³⁹ Hopwood et al., "DNA Typing from Human Faeces," 237.

⁴⁰ Herber and Herold, "DNA Typing of Human Dandruff," 648.

⁴¹ See, for example, *People v. Aylor*, N.Y.L.J., Oct. 1, 2004, at 19 (denying defendants motion to suppress DNA evidence procured from cigarettes offered to defendant in a police interview); Gordon, "DNA Sample Links Man," 5 (describing defendants conviction of car burglary after officer saved cigarette discarded during police interview); Francescani, "Sex Fiend Admits He Killed," 11 (reporting on defendant linked to five murders after police collected saliva on the ground outside of police station, and after defendant refused to provide DNA sample); Rashbaum, "Man Cleared by DNA," 12. For further examples, see Willing, "As Police Rely More," 1A (reporting on abandoned DNA cases in St. Petersburg, Florida, Boston, and New York City); Gosch, "Great-Grandmother's Killer Caught," 5 (describing a defendant linked to murder after police collected a used cigarette discarded during police custody).

licked postage stamps,⁴² envelopes,⁴³ and fingerprints⁴⁴ when nucleated cells presumably transfer to the examined object.

Intact DNA can be analyzed for a long period of time, provided it has not completely degraded due to environmental factors (e.g., heat, humidity, chemical exposure). DNA can be transferred from one object to another (e.g., from victim to suspect, suspect to victim, as well as victim or suspect to an object, object to object, or victim or suspect to a location at a crime scene).⁴⁵ Technical advances in forensic analysis have now made DNA extraction possible from very even very small quantities of an original sample,⁴⁶ down to even a single cell that is invisible to the naked eye. The resulting DNA can be amplified by the polymerase chain reaction (PCR) and then subsequently analyzed⁴⁷ with increasing sensitivity and reliability to determine its origin and ultimately identify its source.

Forensic DNA Analysis Technology

Contemporary forensic DNA analysis utilizes a technique known as Short Tandem Repeat (STR) analysis, which evaluates the presence of specific repeated

⁴² Nelkin and Andrews, “DNA Identification and Surveillance Creep,” 689, 693.

⁴³ See Ho, “Man is Sentenced in ’82,” B1; Johnson, “N.J. Man Convicted,” B1; Nelkin and Andrews, “DNA Identification and Surveillance Creep,” 689, 693.

⁴⁴ van Oorschot and Jones, “DNA Fingerprints from Fingerprints,” 767.

⁴⁵ Lee et al., “Guidelines for the Collection,” 344.

⁴⁶ DNA is contained in blood, semen, skin cells, tissue, organs, muscle, brain cells, bone, teeth, hair, saliva, mucus, perspiration, fingernails, urine, and feces. See National Commission on the Future of DNA Evidence, U.S. Department of Justice, *What Every Law Enforcement*, 2 (noting that “only a few cells can be sufficient to obtain useful DNA information.”). See also Ross, “A Trail of Genetic Evidence,” *supra* note 3 (reporting that 500 picograms to one nanogram is sufficient for a “good” DNA sample).

⁴⁷ Butler, *Forensic DNA Typing*, *supra* note 21, 35.

sequences of DNA when comparing results from two or more samples. The STR methodology is based on variability in the number of tandem repeats at multiple distinct locations (loci) in the genome, enabling scientists to distinguish one DNA sample from another, assuming absence of contamination, DNA degradation, or other artifacts.^{48,49} Because individuals inherit different numbers of repeat units, depending on the genotype of the parents, STR analysis can be used to discriminate between related individuals (except for identical twins) and also those who are not genetically related.⁵⁰

Each STR locus used for human identification exhibits population variation (is polymorphic) as the number of alleles varies from about five to twenty and in frequency in different populations.⁵¹ The strength of STR analysis comes from examining multiple STR loci simultaneously and visualizing the capillary electrophoretic separation pattern of alleles that exist in the sample under analysis. This procedure permits the comparison of sample results to determine whether tested samples from known individuals compare to the results from biological evidence collected at crime scenes. The greater the number of STR regions tested in an individual, the higher the stringency of test for a DNA match.⁵²

⁴⁸ Edwards et al, "DNA Typing and Genetic Mapping," 746-756.

⁴⁹ Gill et al., "The Evolution of DNA Databases," 242-244.

⁵⁰ Martin et al., "A Brief History of the Formation," 225-231.

⁵¹ Norrgard, "Forensics, DNA Fingerprinting, and CODIS," 35. See STR Analysis in National Commission on the Future of DNA Evidence, *Using DNA to Solve Cold Cases*, 6.

⁵² In the United States, thirteen autosomal STR loci are now accepted as the system used for forensic purposes. See Norrgard, "Forensics, DNA Fingerprinting, and CODIS," 1. Given a robust crime scene DNA sample with good data for all thirteen STRs, the likelihood of a person unrelated to the actual perpetrator having a perfect match for all thirteen is typically around one in one billion. By contrast, experimental work with a very robust set of 30 Y-STR loci showed a probability of about 1 in 50,000 for a perfect match. See Hanson and Ballantyne, "A Highly Discriminating 21 Locus," 1-12.

DNA Genealogy, Technology, and Background

DNA fingerprinting, one of the great discoveries of the late 20th century, has revolutionized forensic investigations. Thirty years of progress in forensic DNA analysis, which helps to convict criminals, exonerate the wrongly accused, and identify victims of crime, disasters, and war has resulted in DNA analysis being accepted in countries all over the world as a reliable identification tool. Current standard methods are based on homology to at least thirteen STR⁵³ as well as lineage markers on the Y chromosome⁵⁴ and mitochondrial DNA (mtDNA).⁵⁵ Forensic genetic fingerprinting can be defined as the comparison of the DNA in a person's nucleated cells with that identified in biological matter found at the scene of a crime or with the DNA of another person for the purpose of identification or exclusion. The application of these techniques introduces new evidence to criminal investigations and court cases and continues to help investigators solve cold cases. Thus, DNA serves as a witness to a crime.

Until the introduction of new recently marketed STR testing kits that type over twenty STR markers, the European standard loci consisted of a set of twelve STR markers, and the U.S. CODIS core loci consisted of thirteen markers. Due to partial overlap in the loci typed, together they constitute a standard of eighteen STR markers in total. The probability, using the product rule, that two individuals will have identical markers at each of thirteen different STR loci within their DNA is less than one in one billion. If a DNA "match" occurs between a known suspect and a crime scene stain, the

⁵³ Budowle et al., "CODIS and PCR-based Short Tandem," 73–88.

⁵⁴ Ballantyne et al., "A New Future of Forensic," 208–218.

⁵⁵ Roewer and Parson, "Internet Accessible Population Databases: YHRD and EMPOP."

correct courtroom expression would be that the probability of finding that particular profile (i.e., the crime scene sample profile) in a randomly selected unrelated individual is—at most—one in one billion.⁵⁶

Familial DNA database searching is based on near matches between DNA collected from the scene of a crime and that of a profile of a convicted person in the offender database, which could be derived from a close biological relative of the true perpetrator.⁵⁷ In many countries and in all U.S. states, DNA profiles of those convicted of specified crimes are stored as part of a DNA database. This mandatory requirement is due to a decision by the Supreme Court of the United States, which held that “when officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the police station to be detained in custody, taking and analyzing a cheek swab of the arrestee’s DNA is akin to fingerprinting and photographing, a legitimate police booking procedure”⁵⁸

In *Maryland v. King*, a 5-4 majority with Justice Anthony Kennedy delivering the opinion, the United States Supreme Court held that conducting a DNA swab test as a part of the arrest procedure does not violate the Fourth Amendment because the test serves a legitimate state interest and is not so invasive so as to require a warrant.⁵⁹ In other words, DNA can be taken from an arrestee as a part of the normal booking procedure. As of 2019, twenty-eight states and the federal government now take DNA swabs after arrests

⁵⁶ Jobling et al., *Human Evolutionary Genetics*, 474–497.

⁵⁷ Maguire et al., “Familial Searching: A Specialist,” 1–9.

⁵⁸ Maguire et al., “Familial Searching: A Specialist,” 1–9.

⁵⁹ *Maryland v. Alonzo Jay King, Jr.*, 569 U.S. 435 (2013).

with the aim of comparing profiles to the CODIS database, creating links to unsolved cold cases and to identify the offender.

In addition to government-controlled offender/arrestee DNA databases, many individuals in society freely submit their saliva to various companies in hopes of identifying and locating family members or exploring their biogeographic ancestry. They do this by uploading their DNA results onto publicly accessed websites, which are also open to law enforcement officials who might seek to identify the source of DNA found in crime scenes. This indirect method of kinship analysis has also led to the resolution of cold cases.⁶⁰

The steady growth in the size of forensic and public DNA databases raises issues on the criteria of inclusion and retention and may cast doubts on the efficiency, appropriateness, and privacy of such large personal data collections. In contrast to the past, in some countries, not only serious, but all felony crimes, are typically subject to DNA analysis, generating thousands of DNA profiles, which are stored and regularly searched in local, state, or national DNA databases. When such large datasets are gathered, new data mining procedures based on genetic relationships become feasible.⁶¹

Debate on Public Databases

Activists, genetic database sleuths, and scholars have raised questions regarding privacy associated with publicly accessible national databases. Not only the requirement, but also the appropriateness, of these growing databases is being examined. In spite of its

⁶⁰ Bieber et al., "Finding Criminals through DNA," 1315-1316.

⁶¹ Roewer, "Male DNA Fingerprints Say More," 14-15.

demonstrated success in dozens of high-profile cases, the appropriateness of presenting evidence in a court of law from DNA database searching has been debated in the UK and Germany. For example, “Familial DNA Database Searching” is based on near matches between a sample gathered at the crime scene and the DNA profile of a convicted offender whose profile is stored in the government database. Such close, but not perfect, “matches” could lead investigators to close relatives of the person whose information is housed in the database who, in turn, could be close biological relatives of the person of interest (i.e., the true perpetrator).⁶²

A successful familial search conducted in the UK in 2004 led to the conviction of Craig Harman for manslaughter.⁶³ Harman was convicted because of partial matches of crime scene DNA to that of his brother, whose DNA was already in the UK database. This case also led to the first successful prosecution of an individual identified through familial search techniques after Craig Harman admitted to the manslaughter of Michael Little, a truck driver. Harman threw a brick from the M3 motorway bridge that crashed through the windscreen of Mr. Little’s truck or lorry when he was driving. The brick struck Mr. Little in the chest and triggered a fatal heart attack. Harman, who had no prior criminal record, had left his DNA on the brick. However, he could not be identified through a traditional DNA profile search as he lacked a criminal record and consequently, his DNA profile was not available to UK authorities. But through familial searching, forensic experts traced a close relative who was on police records and detectives were able to use the family link to trace the perpetrator of the crime. Chris Harman was

⁶² Maguire et al., “Familial Searching: A Specialist,” 1–9; Bieber et al., “Finding Criminals through DNA,” 1315-1316.

⁶³ BBC News, “Killer Caught by Relative’s DNA,” at <http://news.bbc.co.uk/>.

arrested and confessed to the crime. Interestingly, familial searching technique had been introduced in the UK only a few months prior to the Harman incident.⁶⁴

Another case in Germany caused German authorities to speed up development of the German DNA Database. In March 1998, authorities found the body of an eleven-year-old girl in a forest in Northern Germany. According to the case report, the girl had been raped and stabbed multiple times. Forensic analysis revealed a sperm stain that could be analyzed for DNA; however, the infancy of the German DNA Database resulted in no matches. The prosecutor determined that conducting an intelligence-led-screen could identify the perpetrator, but intelligence-led-screening is more effective when the subgroup is narrowed. Thus, a perpetrator profile was developed, and it indicated that the offender could be anywhere from eighteen to thirty years old living within a narrow geographic region. In total, about 18,000 males fit this profile description. Local law enforcement issued a request for voluntary reference samples in the form of buccal swabs and found a great degree of cooperation among residents.⁶⁵

More than 11,000 samples were analyzed in police laboratories in Hannover, Berlin, and Magdeburg. In May 1998, one sample yielded a match. An independent analysis in a second laboratory as well as the typing of a second reference sample from the suspect confirmed the results. The DNA profile of the reference samples matched the one derived from the sperm stain at the crime scene. The suspect, a thirty-year-old male living in the area identified in the profile, was arrested and subsequently confessed not only to the murder of the eleven-year-old girl, but also to the killing of another missing

⁶⁴ BBC News, “Killer Caught by Relative’s DNA”; BBC News, “Brick Thrower Jailed over Death”; Maguire et al., “Familial Searching: A Specialist,” 2.

⁶⁵ Wenzel, “ENFSI: Report on Criminal Cases,” 2, 3.

young girl. He was sentenced to life in prison, and the case ultimately led to the setup of the German DNA Database.⁶⁶

German police investigated a separate serial case involving the rape and brutalization of nine women in their homes between 1998 and 2003 in the city of Bremerhaven. DNA analysis confirmed that sperm stains from four of the crimes were identical. The perpetrator wore a mask, limiting the information available to the police. The profile specified the most likely geographical area for the perpetrator was Lehe, a city quarter. Within the geographical area, approximately 2,300 males between twenty-four and forty-six years of age were targeted for voluntary DNA testing; however, the State General Prosecutor deemed the test as illegal and prohibited the German Mass DNA Testing authority (ILS). This decision was subsequently overruled by a local court one month later.

Among the targeted young men, about 100 refused to give a DNA sample. Traditional investigation methods and a court order to collect DNA samples led the police to a thirty-six-year-old suspect who had no alibi for the time when the crime was committed. The DNA sample taken from him yielded a match to the ones collected from the crime scenes. The suspect ultimately confessed to four rapes and was sentenced to nine years in prison in December 2005.⁶⁷ DNA testing ultimately resolved a cold case where traditional police investigative techniques had not yielded results.

Civil rights and liberties are crucial for democratic societies, and plans to extend forensic DNA databases to whole populations need to be addressed. In the UK, Alec

⁶⁶ *Supra* note 65.

⁶⁷ *Supra* note 65.

Jeffreys has questioned the way police collect DNA profiles, holding not only convicted individuals but also arrestees without conviction, suspects cleared in an investigation, or even innocent people never charged with an offense.⁶⁸ Jeffreys has also criticized large national databases, such as the National DNA Database (NDNAD) of England and Wales, noting that they are likely skewed socioeconomically. Due to the UK's Criminal Justice Act of 2003, DNA profiles of suspects cleared in an investigation can be held indefinitely on NDNAD, based on the assumption that they will offend in the future. This number has been increasing and includes hundreds of thousands of individual profiles. On this, Jeffreys writes, "this extension of NDNAD to a subset of the general population that is likely to be skewed socioeconomically and ethnically raises issues of civil liberties and genetic discrimination."⁶⁹

According to a report by *GeneWatch*, in Germany, almost two-thirds of the German DNA database matches provided are related to theft, whereas fewer than 3 percent are related to rape and murder.⁷⁰ Since its implementation in 1998, the central German DNA database known as Bundeskriminalamt (BKA) has expanded considerably and currently maintains the DNA profiles of 920,000 individuals. However, only 190,000 of those profiles are samples derived from crime scenes, meaning 730,000 of them from individuals who have never been documented for criminal activity.

According to German law, the police are permitted to store DNA profiles of those accused or convicted of major offenses. Since its reform in 2005, the new German law

⁶⁸ Jeffreys, "Genetic Fingerprinting," 1035–1039.

⁶⁹ Jeffreys, "Genetic Fingerprinting," 1038.

⁷⁰ Schultz, "Stop the DNA Collection Frenzy," at <http://www.councilforresponsiblegenetics.org/>.

counts repeated minor offenses cumulatively, ultimately allowing them to count collectively as a major offense. On these legal grounds, the police have been requesting DNA profiles of those accused of theft and other minor offenses. Although the German public believes that DNA profiles are utilized for capital crimes such as murder and rape, the BKA indicates differently. The majority of the DNA matches reported by BKA are for minor offenses.⁷¹

The National DNA Database (NDNAD) of England and Wales was established in April of 1995 and has since grown to be the largest per capita DNA database in the world. The growth in the collection and retention of DNA profiles in England and Wales has been driven by legislative changes⁷² and the Home Office DNA Expansion Programme (2000–2005), which financed £240 million to support the use of DNA profiling in crime investigation.⁷³ By March 2012, there were approximately 5.95 million individuals' DNA profiles and 405,000 crime scene sample profiles retained in the NDNAD⁷⁴. The size of the NDNAD and the fact that related genetic material is retained has led to claims of the NDNAD being a vital tool in the investigation and detection of crime and counterclaims that the consequent invasion of privacy and personal genetic identity outweighs its efficacy in crime detection. These issues were brought to fore by

⁷¹ *Supra* note 60.

⁷² Criminal Justice and Public Order Act (1994); Criminal Evidence Act (1997); Criminal Justice and Police Act (2001); Criminal Justice Act (2003); Serious Organised Crime and Police Act (2005).

⁷³ Home Office, "DNA Expansion Programme 2000–2005," at <http://www.statewatch.org/news/2006/jan/uk-DNA-database.pdf>.

⁷⁴ National Policing Improvement Agency, NDNAD Statistics, at <http://www.npia.police.uk/en/13338.htm>.

the cases of *R (S) and R (Marper) v. The Chief Constable of South Yorkshire* (2004)⁷⁵ and *S and Marper v. The United Kingdom* (2008).⁷⁶

In each of those cases, the contention of the appellant was that the retention of DNA profiles and DNA samples breached the individuals' rights to privacy as neither was convicted of an offense. The South Yorkshire Police contested this view, and the appeals were subsequently dismissed in a 2002 judgment in the Court of Appeal. S and Marper were granted the right to appeal to the Grand Chamber of the European Court of Human Rights (ECtHR) and, in December 2008, the ECtHR ruled that the "blanket and indiscriminate" nature of the UK Government's policy on the retention of DNA profiles and samples in England and Wales, regardless of the age of the offender, the seriousness of the offence, or whether the individual had been charged or convicted, was a breach of the right to privacy (Article 8) of the European Charter of Human Rights.

Following this decision, the UK Government conducted a review and comparison of its DNA retention policy with those of other jurisdictions, notably that of Scotland. The UK Government amended the rules on the retention of DNA profiles and DNA samples for those not convicted of an offense or those against whom investigative or judicial proceedings were discontinued for one reason or another. However, the UK Government has gone much further since the S and Marper cases; the Protection of Freedom Act (2012) allows DNA samples to be retained for a maximum period of six

⁷⁵ *R (S) and R (Marper) v. Chief Constable of South Yorkshire* (2004) UKHL 39; 4 All ER 193.

⁷⁶ *S and Marper v. The United Kingdom* – 30562/04 and 30566/04 (2008) ECHR 1581 (4 December 2008).

months to ensure a full DNA profile is created for inclusion in the NDNAD and to allow for re-examination and re-analysis if necessary.⁷⁷

In 2012, the Protection of Freedoms bill brought changes to the UK database, following a major defeat at the European Court of Human Rights in 2008. These removed profiles belonged to individuals without any prior criminal record. Thereafter, under the Protection of Freedoms Act of 2012, DNA samples held in the national database were targeted to be destroyed. The UK Government also indicated that “legacy” samples (from nearly six million swabs taken) that were held by forensic science suppliers were to be destroyed within 12 months of implementation of the legislative instrument. By May 2013, 1.1 million profiles out of a total of almost seven million were destroyed from the NDNAD, but some UK-based scholars were not in favor of the destruction.

One can argue that the latter decision could negatively impact the ability of the UK police to deliver an effective familial search service. Under the new regulations, the familial search process can still be used to generate the appropriate screened or unscreened candidate lists. The ability to utilize rapid genetic analysis may be compromised by this decision. At present, the stored biological material (buccal swabs) from individuals in the potential candidate lists can be used for quick Y-STR analysis without contacting those individuals, and it can be argued that their personal freedom will suffer minimal intrusion because they will have no knowledge of the analysis.

In the future, the police will have to decide whether to trace and interview some or all of those individuals identified by the familial search process and seek a second, volunteered DNA sample for Y-STR analysis. The outcomes of such a policy change are

⁷⁷ Protection of Freedoms Act 2012, Chapter 1 §14 (5), at <http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted>.

unknown. Individuals might refuse to supply samples and true perpetrators and their relatives could be alerted by others when police formally begin to request to supply a sample. On the other hand, it might simply be prohibitively expensive for the police to trace, interview and sample potentially hundreds of individuals to find the true perpetrators(s).

The Prüm Convention is a treaty signed on May 27, 2005, by Austria, Belgium, France, Germany, Luxembourg, the Netherlands, and Spain in the town of Prüm in Germany, and which subsequently became open to all members of the European Union. The Convention was adopted to enable all signatories to exchange data from DNA, fingerprints, and vehicle registration within the European Union (EU) with the goal of cooperating against terrorism.⁷⁸ Following the Prüm Convention in 2005, the incoming government of Portugal proposed creating a DNA database containing samples from every Portuguese citizen. Portuguese government law specified that samples had to be voluntarily provided and would be permanently held unless a revocation of consent was exercised by the donor.⁷⁹ According to the Portuguese government,

The DNA profiles collected from volunteers are to be preserved for an unlimited time and removed only in the case of explicit revocation of the previously given consent. The collection of samples from volunteers is to be made with free, informed and revocable consent (article 18.1a-b of law 5/2008) and following a sample collection request in writing, which must be addressed by the volunteer to the National Institute of Forensic Medicine (no. 2 of article 6 of Law 5/2008).

The impetus in creating such a database in Portugal was to cooperate with the agreement of the Prüm Convention and address a growing concern of increasing crime

⁷⁸ Council of the European Union, Treaty Prüm, at <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf>.

⁷⁹ Machado and Silva, “Would You Accept Having,” see Introduction 133.

and the possibility of terrorism brought about through cross border migration as the European Union boundaries become increasingly porous. Therefore, to find suspects and bring them to justice speedily, exchange of genetic information through mutual accessibility of national databases was sought by all European Union member states.⁸⁰

In their study, Helena Machado and Susana Silva examined public views of Portuguese residents on issues related to the proposed DNA database.⁸¹ Data were collected from 628 individuals in Portugal through an online survey and analyzed for respondents' willingness to voluntarily submit a sample of their DNA for "profiling and inclusion in the National Forensic DNA database." Participants were asked to share reasons for their decisions. Upon analysis of their questionnaire, Machado and Silva found that a quarter of respondents were against the idea and that the degree of unwillingness directly correlated with increasing age and education. The higher the age and education, the greater was the aversion to voluntarily give up their DNA to be included in the National NA database. However, a majority were willing to have their DNA in a centralized database affirming the potency of forensic DNA technologies and suggesting that civil liberties and human rights were willing to be relegated in favor of protecting the individual and society from crime. The authors wrote,

The DNA profiles collected from volunteers are to be preserved for an unlimited time and removed only in the case of explicit revocation of the previously given consent. The collection of samples from volunteers is to be made with free, informed and revocable consent (article 18.1a-b of law 5/2008) and following a sample collection request in writing, which must be addressed by the volunteer to the National Institute of Forensic Medicine (no. 2 of article 6 of Law 5/2008).⁸²

⁸⁰ *Supra* note 62; Machado and Silva, "Would You Accept Having," 133.

⁸¹ Machado and Silva, "Would You Accept Having," 132-136.

⁸² Machado and Silva, "Portuguese Forensic DNA Database," Chapter 11.

According to Portuguese Law, the volunteer is someone who wishes to donate a sample (Art. 6.1, Law 5/2008). The DNA profiles collected from volunteers are to be preserved for an unlimited time and removed only in the case of explicit revocation of the previously given consent. The collection of samples from volunteers is to be made with free, informed, and revocable consent (Article 18.1a-b, Law 5/2008) and following a sample collection request in writing, which must be addressed by the volunteer to the National Institute of Forensic Medicine (No. 2, Art. 6, Law 5/2008).⁸³

The Portuguese DNA database was formally created under legislation passed in 2008 and combines the purposes of civil identification and criminal investigation.⁸⁴ The custodian of the DNA database is the Ministry of Justice, while the National Institute of Legal Medicine (NILM) is the institution responsible for processing the data (samples and profiles) and for communicating the results of analyses to the competent judicial authorities. Although the original intention was to collect samples from the entire Portuguese population, the Portuguese government limited the database to criminals as had been done in many other European countries and elsewhere.⁸⁵

A recent article published in United States-based *Science* magazine by Joly et al. raises questions on risks associated with the call for a new, mandatory, publicly accessible “forensic database for DNA information” by Hazel et al.⁸⁶ In their view, Hazel

⁸³ Machado and Silva, “Would You Accept Having,” 132-136.

⁸⁴ *Diário da República*, “Law 5/2008 Approves the Creation,” 962-968.

⁸⁵ Machado and Silva, “Portuguese Forensic DNA Database,” chapter 11.

⁸⁶ Joly et al., “Risks of Compulsory Databases,” 938.

et al.'s proposed database⁸⁷ would compile DNA information obtained from newborns and would ultimately benefit society by correcting issues in the current database system, including “discrimination, mismanagement, misuses of genetic information and questionable search practices.” However, Joly et al. disagree with this hypothetical notion and present a different point of view. Rather than leveling the playing field, Joly et al. argue that a compulsory database would place minority groups at an additional disadvantage and further exacerbate already “strained” relationships with governmental agencies. Joly et al. are of the opinion that “creating compulsory genetic databases will not make the system more humane for minority group or improves strained relationships with government agencies. Better regulation of existing structures and added considerations for vulnerable groups might be a more effective strategy.”⁸⁸ Therefore, a more viable solution is to improve management of existing databases with special considerations added to help those in society who lack powerful voices, according to Joly et al.⁸⁹

To reinforce their point of view, Joly et al. cite an example of how change was brought about through the collective voice of public opinion. In 2015, the implementation of a law requiring a compulsory national database in Kuwait was jointly criticized by human rights groups as an impediment to an individual’s right to privacy.⁹⁰ Subsequently,

⁸⁷ Hazel et al., “Is It Time for a Universal,” 898-900.

⁸⁸ *Supra* note 87.

⁸⁹ *Supra* note 87.

⁹⁰ Human Rights Watch, “Kuwait: New Counterterrorism Law,” at <https://www.hrw.org/news/2015/07/20/kuwait-new-counterterrorism-law-sets-mandatory-dna-testing>; UN Human Rights Committee, “Concluding Observations: Kuwait,” at <https://www.refworld.org/publisher,HRC,CONCLOSURES,KWT,3df36be44,0.html>.

the law was invalidated by the Kuwaiti constitutional court.⁹¹ A concern voiced by Joly et al. centers around the cost of developing a genetic database of the type proposed by Hazel et al.⁹² Such a database would be potentially “intrusive for everyone” and would “increase the risk of abusive usage of genetic information,” caution Joly et al.⁹³ Not only that, such a database could potentially worsen the “climate of mistrust”⁹⁴ and “negatively” impact public’s view of genetics. The authors are especially wary of analogizing compulsory collection of genetic information from newborns and its subsequent incorporation into the database with public health screening, as Hazel et al. have suggested. They characterize this as “tendentious and unhelpful.”⁹⁵ Such databases were meant to serve the public need with early identification and treatment newborns for serious congenital genetic disorders like phenylketonuria (PKU) which is the best way that such a database can be useful, according to Joly et al.⁹⁶

Hazel et al. responded to Joly et al. while holding their ground on their support for the construction of universal genetic databases.⁹⁷ While agreeing with Joly et al. that the idea of building universal forensic databases is associated with risks and has encountered firm disapproval by some, Hazel et al. cited others in the field who stand with them on

⁹¹ *Supra* note 87; Joly et al., “Risks of Compulsory Databases,” 938.

⁹² *Supra* note 87. Forensic Genetics Policy Initiative, “Establishing best practice,” at <http://dnapolicyinitiative.org/wp-content/uploads/2017/08/BestPractice-Report-plus-cover-final.pdf>.

⁹³ *Supra* note 87.

⁹⁴ Madden and Rainie, “Americans’ Attitudes about Privacy,” at <https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

⁹⁵ Hazel et al., “Is It Time for a Universal,” 898-900.

⁹⁶ *Supra* note 87.

⁹⁷ Hazel et al., “Is It Time for a Universal,” 898-900, in response to Joly et al., “Risks of Compulsory Databases,” 939.

the advantages of having a universal database.⁹⁸ Hazel et al. pointed out that the impetus of their “Policy Forum” is to call to attention the imperfections that are associated with the current government run forensic databases, such as information stored in government databases like GEDmatch.⁹⁹ They asserted that law enforcement access to information stored in underregulated GEDmatch and private databases like FamilyTree is “haphazard” even though they have free open-access to the genetic information and are increasingly “exploiting” the genetic information that is stored in them.¹⁰⁰ Hazel et al. also expressed concern over the loss of control over privacy as national and state law enforcement agencies move towards expanding government managed databases.¹⁰¹ They cited the use of a new invention—the portable “Rapid DNA”—as an example of unfettered access to DNA analysis by police stations, which was once at the hands of only qualified laboratories.¹⁰²

Hazel et al. voiced their support to the idea of building a compulsory national database that is regulated and inaccessible, requiring authorized permission from its participants before use.¹⁰³ They noted that such a database would be “rigorously monitored and equitably administered” when compared to those databases carrying

⁹⁸ Williamson and Duncan, “Commentary,” 585-586; Kaye and Smith, “DNA Identification Databases,” 413, 424; Dedrickson, “Universal DNA Databases,” 637-647.

⁹⁹ *Supra* note 99.

¹⁰⁰ Molteni, “The Future of Crime Fighting,” at <https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/>; Haag, “Family TreeDNA Admits,” at <https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html>.

¹⁰¹ *Supra* note 99.

¹⁰² *Supra* note 99.

¹⁰³ Hazel et al., “Is It Time for a Universal,” 898-900, in response to Joly et al., “Risks of Compulsory Databases,” 939.

information collected from a subset of the population who are presumably convicted offenders and their relatives. This type of criticism seems to echo the sentiments of Sir Alec Jeffreys, who has expressed his support for creating a national database system in the UK, albeit calling for rigorous monitoring.¹⁰⁴

Use of DNA in Law Enforcement

Often, law enforcement officials must rely on DNA that has been inadvertently shed by victims and suspects to associate individuals with a crime directly or to determine their presence at the scene of a crime. Similarly, victims can also be tested for the presence of suspect DNA to determine if the suspect and victim were in physical contact. Police can obtain discarded DNA from suspects not only from crime scenes, but also through indirect means by taking samples from discarded items (e.g., clothing, food, eating utensils) with a suspect's DNA on it. In situations where the police have not accumulated enough probable cause for a search warrant, they may follow that suspect and clandestinely collect potential sources of their DNA that can be found on discarded personal items or substances on which their saliva or shed skin may have transferred.

Police have been also known to trick persons of interest into involuntarily shedding their DNA by offering them a soda or a cigarette. In *State v. Athan*, the police devised a creative method to lure John Athan into giving them a sample of his DNA to solve a twenty-year-old cold case. The police had long suspected Athan in a 1982 murder of a thirteen-year-old girl in Seattle, Washington, but Athan had since moved out of state and was residing in New Jersey. Posing as a fictitious law firm, the police sent a letter to

¹⁰⁴ Jeffreys, "Genetic Fingerprinting," 1035-1039; *supra* note 68; *supra* note 99.

Athan to entice him into join a class action lawsuit involving the recovery of overcharged parking tickets.¹⁰⁵ Since Athan was eager to join this lawsuit, he sent back a signed authorization form in an envelope provided by the police after licking the flap to seal it shut.¹⁰⁶

Unbeknownst to Athan, the police now had access to a sample of his DNA since it could be extracted from the saliva that he had left on the sealed envelope flap. Working with forensic laboratories, the police were able to determine that the DNA on the envelope matched the one that was found in the bodily fluids of the victim. With this information as potent evidence against Athan, law enforcement could show that he had physical contact with the thirteen-year-old girl. Subsequently, Athan was convicted for second degree murder.¹⁰⁷

¹⁰⁵ Gillespie, "Need for Greed Ends," A20 (reporting that police around the country have put suspects under surveillance in hopes that they might discard a cigarette or wad of gum from which DNA could be drawn).

¹⁰⁶ Ho, "Man Is Sentenced in '82 Killing," B1.

¹⁰⁷ See Johnson, "N.J. Man Convicted," B1. In Athan's criminal prosecution, neither side disputed that "one's cells sloughed in public in the normal course of daily living are not entitled to constitutional protection." See *State v. Athan*, No. 03-1-06338-6, slip op. at 4 (order on defendant's motion to suppress DNA evidence) (on file with author). Rather, Athan argued that the police violated his rights under the Washington Constitution, which provides greater privacy rights than does the Fourth Amendment of the Federal Constitution. The trial court rejected these claims. In 2007, the Washington State Supreme Court held that Athan abandoned any expectation of privacy he may have had in his saliva when he unintentionally but voluntarily mailed to detectives an envelope he had licked. See *State v. Athan*, 160 Wn.2d 354, 158 P.3d 27 (2007).

Chapter II.

Fourth Amendment Jurisprudence

The Fourth Amendment to the U.S. Constitution guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated. . . .”¹⁰⁸ The nature and scope of this protection against an intrusion on the intangible genetic privacy was certainly not a consideration when the Amendment was ratified on December 15, 1791, and it is not readily apparent in the amendment’s original text. As a practical matter, the question that should be considered is why police choose to collect abandoned DNA when looking for incriminating evidence. It seems that there are at least six possible reasons:

1. Abandoned DNA is easy and cost effective¹⁰⁹ to collect. These DNA samples are available from anyone and can be collected without the targeted person’s knowledge and, therefore,
2. Abandoned DNA can be obtained without any objection or resistance from the owner. A suspect may refuse to provide a sample, and the police have no other choice except to collect passively by waiting for a suspect to discard a smoked cigarette or drinking cup or to spit on the floor.¹¹⁰

¹⁰⁸ U.S. Const. amend. IV.

¹⁰⁹ While easy to collect, the actual analysis of the samples can be costly, depending on the difficulty of the case. Analysis for a murder case may cost upwards of \$10,000, as compared to \$500 in a rape case. See Willing, “DNA’s Success in Crime-Fighting,” A1.

¹¹⁰ See, for example, *New York Law Journal*, “People v. Anthony Ayler,” 19 (denying defendant’s motion to suppress DNA evidence procured from cigarettes offered to defendant in a police interview);

3. Current techniques used by forensic laboratories are at a level of sensitivity such that only a small amount of saliva, blood, or hair is required. The police need only obtain a minute tissue sample.
4. The police may have no more than a speculation about the suspect and lack a firm basis to obtain a warrant to collect the DNA.
5. Manpower resources are limited, and logistics of obtaining a sample are complicated in order to conduct a detailed investigation.
6. Police suspect someone in a “cold” case where the crime occurred many years ago and in which a prior investigation produced no solid leads.

Scholarly Conclusions and Case Law

Arguments regarding law enforcement’s harvesting and subsequent analysis of inadvertently shed (i.e., abandoned) DNA have been examined in the context of Fourth Amendment jurisprudence and whether it provides ample constitutional protection of personal privacy. Two scholars in the field have contributed to the debate and ostensibly reached different conclusions.

David Kaye is not a proponent of granting a special status to DNA regarding its reasonable expectation of privacy.¹¹¹ He compares abandoned DNA analysis to

Gordon, “DNA Sample Links Man,” 5 (describing defendant’s conviction of car burglary after officer saved cigarette discarded during police interview); Francescani, “Sex Fiend Admits He Killed,” 11 (reporting on defendant linked to five murders after police collected saliva on the ground outside of police station, and after defendant refused to provide DNA sample); Rashbaum, “Man Cleared by DNA,” 12 (same). For further examples, see Willing, “As Police Rely More,” 1A (reporting on abandoned DNA cases in St. Petersburg, Florida, Boston, and New York City); Gosch, “Great-Grandmother’s Killer Caught,” 5 (describing a defendant linked to murder after police collected a used cigarette discarded during police custody).

¹¹¹ See Kaye and Smith, “DNA Identification Databases,” 413, 424.

fingerprint analysis and cautions that courts must not be distracted by the occasional deception involved in harvesting DNA that has been shed from the body.¹¹² Otherwise, the courts would be indulging in “genetic exceptionalism,” writes Kaye. In Kaye’s view, fingerprints lack Fourth Amendment protections because they are constantly exposed to public scrutiny,¹¹³ and, therefore, one cannot hold any reasonable expectation of privacy with regard to such publicly available knowledge.¹¹⁴ He questions whether STR DNA analysis can reveal anything more about a person than mere nametag data and, therefore, asserts that DNA does not carry personal information.

Conversely, Elizabeth Joh refers to obtaining DNA surreptitiously as “covert involuntary sampling” and rejects the notion of DNA as the equivalent of collecting trash left on a curbside with a free for all privilege.¹¹⁵ Joh questions the appropriateness of a Fourth Amendment abandoned-property or “trash” equivalence to covert DNA collection by the police and states that “the Fourth Amendment’s protections appear to fall short of

¹¹² Kaye, “The Science of DNA Identification,” 62; Kaye, “Science Fiction and Shed DNA,” 409, 420.

¹¹³ This rationale has been extended to hair samples as well. See *Coddington v. Evanko* (holding that “the cutting of one’s hair for the purpose of obtaining a sample does not constitute a search under the Fourth Amendment.”). *Coddington* relied upon the Third Circuit’s prior precedent in *Mills*, in which the court concluded “that there is no greater expectation of privacy with respect to hair that is on public display than with respect to voice, handwriting or fingerprints.” In re *Grand Jury Proceedings (Appeal of Mills)*. See also Colb, “Is Your Scalp a Constitution-Free Zone?” at <http://writ.news.findlaw.com/colb/20041117.html> (arguing that *Coddington* and *Mills* are “wrong as a matter of logic” and that *Coddington* “misinterprets” Fourth Amendment law).

¹¹⁴ See Kaye and Smith, “DNA Identification Databases,” *supra* note 49, 432 (“If the Constitution allows the police to keep a fingerprint or a photograph as a biometric identifier . . . then it is hard to see why they cannot keep a DNA profile if it is properly limited to ‘vacuous’ loci”); cf. *Patterson v. State* (“The view that DNA analysis is no different than traditional fingerprinting is becoming less palatable. DNA analysis provides unprecedented access into an individual’s future physical and psychological health, the health of close relatives, and insight into paternity issues.”).

¹¹⁵ Joh, “Reclaiming ‘Abandoned’ DNA,” 857, 882.

providing a constitutional basis from which to challenge abandoned DNA collection of DNA.”¹¹⁶

Evaluating other possible analogies of inadvertently shed DNA to fingerprints, human waste, trash, hair, and body parts are interpretative mechanisms that do not address “what is important about genetic information,” according to Joh.¹¹⁷ Thus, Joh argues that the deficiencies in these analogies “make the case for genetic exceptionalism” and that DNA falls under a unique category that is incapable of abandonment and merits its own analysis without comparison to other body parts or common trash.¹¹⁸

The Fourth Amendment’s prohibition on unreasonable searches and seizure requires a court to first determine whether a search or seizure has taken place at all.¹¹⁹ The case, *Katz v. United States*, 389 U.S. 347 (1967) resulted in a landmark decision by the U.S. Supreme Court where the Court redefined what establishes searches and seizures with respect to the protections of the Fourth Amendment to the U.S. Constitution.¹²⁰ Charles Katz, a resident of Los Angeles, California, had been involved in sports betting for many years.¹²¹ In February 1965, Katz used a public telephone booth near his apartment on Sunset Boulevard to convey his gambling handicaps to bookmakers in Boston and Miami.¹²² The Federal Bureau of Investigation (FBI) had begun

¹¹⁶ Joh, “Reclaiming ‘Abandoned’ DNA,” *supra* note 55, 868.

¹¹⁷ Joh, “Reclaiming ‘Abandoned’ DNA,” *supra* note 55, 882-883.

¹¹⁸ Joh, “Reclaiming ‘Abandoned’ DNA,” 869.

¹¹⁹ U.S. CONST. amend. IV.

¹²⁰ LaFave, *Search and Seizure: A Treatise*, § 2.1(b), p. 576.

¹²¹ Schneider, “Katz v. United States: The Untold Story,” 13.

¹²² Schneider, “Katz v. United States: The Untold Story,” 13.

investigating him and was recording his conversations covertly with a listening device attached outside the phone booth. The FBI arrested Katz and charged him with eight counts of knowingly transmitting wagering information over telephone across U.S. states, which is a federal crime under 18 U.S.C. § 1084.¹²³ Katz was tried in the U.S. District Court for the Southern District of California¹²⁴ where the judge ruled that the FBI recordings were admissible and Katz was convicted based on the evidence they provided the police.

Katz subsequently appealed his conviction to the U.S. Court of Appeals for the Ninth Circuit. In November 1966, a three-judge panel of the Ninth Circuit affirmed Katz's conviction, ruling that because the FBI's eavesdropping device did not physically penetrate the telephone booth's wall and had been placed outside the phone booth. Therefore, no Fourth Amendment search occurred, based the ruling by the U.S. Court of Appeals. As such, the FBI did not need a search warrant to place the device outside the phone booth and Katz right to privacy had not been violated by the government.¹²⁵ Katz then appealed the U.S. Court of Appeals ruling to the U.S. Supreme Court, which agreed to hear his case and granted *certiorari*.¹²⁶ The U.S. Supreme Court heard oral arguments on the case in October 1967 and delivered their decision on December 18, 1967. The

¹²³ LaFave, *Search and Seizure: A Treatise*, § 2.1(b), p. 576.

¹²⁴ *Note*: The Southern District was split in 1966, and today the case would fall under the United States District Court for the Central District of California.

¹²⁵ LaFave, *Search and Seizure: A Treatise*, § 2.1(b), p. 576.

¹²⁶ LaFave, *Search and Seizure: A Treatise*, § 2.1(b), pp. 576-577.

Supreme Court of the United States issued a 7 to 1 decision in favor of Katz that invalidated the FBI investigators' search.¹²⁷

In *Katz v. United States*, U.S. Supreme Court Associate Justice Harlan expressed the “reasonable expectation of privacy” test that provides a modern analytic framework in cases that involve a breach of privacy.¹²⁸ Investigative police activity constitutes a “search” for Fourth Amendment purposes only if the person claiming an illegal search exhibits both an actual expectation of privacy and one that “society is prepared to recognize as ‘reasonable’.”¹²⁹ Likewise, the U.S. Supreme Court has stated that police collection of physical evidence constitutes a “seizure” if it is a “meaningful interference with an individual’s possessory interests in that property.”¹³⁰ The acquisition by force of a person’s blood or urine, too, is considered by the courts a seizure because it is “a meaningful interference with [one’s] possessory interest in his bodily fluids.”¹³¹

In contrast, where suspects “knowingly expose” items to public view, the Court has held that collection of such evidence by the police falls outside the Fourth Amendment’s protections.¹³² In such cases, police involvement is neither a search nor a

¹²⁷ Schneider, “Katz v. United States: The Untold Story,” 13.

¹²⁸ See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

¹²⁹ See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

¹³⁰ *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

¹³¹ *Skinner v. Ry. Labor Executives Ass. ’n*, 489 U.S. 602, 618 n.4 (1989). In *Skinner*, however, the Court noted that it was “not necessary . . . to characterize the taking of blood or urine samples as a seizure of those bodily fluids, for the privacy expectations protected by this characterization are adequately taken into account by our conclusion that such intrusions are searches.” *Id.*; see also *Schmerber v. California*, 384 U.S. 757, 767 (1966) (“[T]he administration of the blood test in this case was [not] free of the constraints of the Fourth Amendment. Such testing procedures plainly constitute searches of ‘persons’ and depend antecedently upon seizures of ‘persons,’ within the meaning of that Amendment”).

¹³² *Katz v. United States*, 389 U.S. 347, 351 (1967).

seizure for Fourth Amendment purposes.¹³³ Thus, the Katz ruling serves as a precedence for cases related to the governmental interference of an individual's privacy continues to provide a frame of reference for deciding on cases that involve abandoned DNA and an individual's right to privacy even though DNA was never abandoned by Katz and that in itself was not an issue upon which the *Katz v. United States* decision was based.

Because it is grounded in physical boundaries, the Fourth Amendment focuses more on the physical boundaries of persons and places than it does on the quantity of information that may be found within them. The Fourth Amendment's prohibition on unreasonable searches and seizures requires a court first to determine whether a search or seizure has taken place at all. In *Katz v. United States*, Justice Harlan articulated the "reasonable expectation of privacy" test that provides the modern analytic framework. Police activity constitutes a "search" for Fourth Amendment purposes only if the person claiming an illegal search exhibits both an actual expectation of privacy and one that "society is prepared to recognize as 'reasonable.'"¹³⁴ In their analyses, both Kaye and Joh use *Katz v. United States*¹³⁵ as a litmus test to evaluate a reasonable expectation of privacy, with both ultimately concluding that Fourth Amendment jurisprudence does not provide an individual constitutional protection from surreptitious harvesting of abandoned DNA.

Courts have consistently vetoed Fourth Amendment protection against surreptitiously harvesting abandoned DNA of putative suspects. Typically, U.S. courts

¹³³ See, e.g., *Abel v. United States*, 362 U.S. 217, 241 (1960) (finding that government collection of items left in hotel room wastepaper basket was permissible because to defendant such items were "bona vacantia," or ownerless goods).

¹³⁴ *Katz v. United States*, 389 U.S. 347, 351 (1967).

¹³⁵ *Katz v. United States*, 389 U.S. 347, 361 (1967).

have found that, regardless of how, where, or why it is left behind, suspects cease to have all rights to their DNA once abandoned for two main reasons. First, once discarded, an item bearing an individual's DNA (e.g., in saliva, hair, or blood) becomes separated from the body, and it is unlikely that the sample is obtained by coercion. Second, a publicly discarded item is likened to trash and is, therefore, available to the public on a first-come, first-served basis. Consequently, the public cannot have any expectation of privacy on the item in which their DNA was found, whether it is a cigarette butt, a drinking cup, or saliva. However, by focusing on the reasonable expectation of privacy of the discarded item, virtually no court has yet considered granting privacy either to the person's DNA itself or the nature and degree of the person's genetic privacy rights by leaving a body part (e.g., skin, blood, or hair) behind.

People v. Sigsbee

A comprehensive opinion on the Fourth Amendment's implication of secretive harvesting of a suspect's DNA by law enforcement officials can be found in *People v. Sigsbee*.¹³⁶ In 1975, Donald Sigsbee was a suspect in the murder of a 19-year-old woman, Regina Reynolds, whose body was discovered in a remote landfill area in upstate New York.¹³⁷ Even though Sigsbee's business cards were found near the body, which provided some evidence, the police did not have enough for probable cause required to obtain a search warrant in order to get a sample of the suspect's blood or saliva for DNA analysis.

¹³⁶ *People v. Sigsbee*, D057191 (Cal. Ct. App. Sep. 6, 2011).

¹³⁷ *Oneida Daily Dispatch*, "Convicted Murderer Donald Sigsbee," at <https://www.oneidadispatch.com/>.

Without probable cause, a search warrant, and Sigsbee's DNA, the case remained unresolved for almost three decades.

In 1975, forensic DNA testing was not an available option. It would take another twenty-eight years before the police could gather evidence to try and convict Sigsbee for the murder.¹³⁸ Once DNA analysis was available as an option, the police sought to solve this cold case. They followed Sigsbee to a Wendy's fast food restaurant and watched him eat a meal and discard his used soft drink cup and straw.¹³⁹ After Sigsbee left the restaurant, the police retrieved the cup and straw from the trash and submitted them for forensic DNA testing.¹⁴⁰

At trial, Sigsbee's motion to suppress the DNA evidence collected from the abandoned drinking straw was denied by the Onondaga County (NY) Court trial court. The court held that the Fourth Amendment protection of privacy did not apply because Sigsbee had voluntarily abandoned the straw.¹⁴¹ The court document read,

When the defendant discarded the drinking straw, he also discarded any expectation of privacy in the DNA evidence on the straw. While it is unlikely that the defendant believed that he was discarding bodily fluids that would show his DNA profile, nonetheless, by discarding the cup and straw into the trash receptacle, he relinquished any expectation of privacy concerning those items themselves or any bodily fluids contained on them.... The scientific analysis of the straw does not involve any further search and seizure of the defendant's person or property and does not, therefore, involve any violation of the defendant's constitutional rights to be free from unlawful searches and seizures.¹⁴²

¹³⁸ *People v. Sigsbee*, D057191 (Cal. Ct. App. Sep. 6, 2011), 8.

¹³⁹ *People v. Sigsbee*, D057191 (Cal. Ct. App. Sep. 6, 2011), 9.

¹⁴⁰ *People v. Sigsbee*, D057191 (Cal. Ct. App. Sep. 6, 2011), 9-10.

¹⁴¹ *People v. Sigsbee*, D057191 (Cal. Ct. App. Sep. 6, 2011), 28.

¹⁴² *People v. Sigsbee*, D057191 (Cal. Ct. App. Sep. 6, 2011), 31-32. The Sigsbee court also made an effort to analyze the possibility of Sigsbee having an expectation of privacy in his bodily fluids. Unlike escaping heat from one's home, the voluntary discarding of a cup and straw in a public restaurant involved

Commonwealth v. Bly

Jeffrey Bly, a gang leader who was notorious for intimidating and silencing witnesses against him, was accused of killing Boston's anti-gang prosecutor Paul McLaughlin.¹⁴³ On Sept. 25, 1995, it was alleged that Bly shot McLaughlin in the head at point-blank range after jumping out from behind bushes and grabbing the prosecutor as he was getting into his 1982 Toyota at a West Roxbury railway station after completing work at the DA's office. On the following day, McLaughlin was set to begin prosecuting a carjacking case against Bly, who police say had recently failed in a conspiracy to kill the key witness against him.¹⁴⁴

In Massachusetts, the murder of McLaughlin was the first-ever homicide of a prosecutor and, consequently, created tremendous anxiety in the criminal justice system. The case against Bly was advanced through a combination of eyewitness accounts and DNA evidence.¹⁴⁵ The court case consisted of testimony from law enforcement's conversations with some of Bly's former gang allies and from two women who heard him boast about the crime. Another witness testified she saw Bly near the scene of the crime around the time of the murder but hesitated to come forward because she did not want to

a conscious and intentional act, which affirmatively demonstrated the relinquishment of any expectation of privacy that one may have had in those items. The loss of heat from one's home, for the most part, does not constitute a conscious, intentional, or voluntary act of the owner of the home. The court then went on to reject more directly any theory that Sigsbee had a reasonable expectation of privacy in his bodily fluids.

¹⁴³ *Commonwealth v. Bly*, 862 N.E.2d 341.

¹⁴⁴ *Commonwealth v. Bly*, 862 N.E.2d 341. See also, Howland, "Inmate Charged in Prosecutor's 1995 Murder," at <https://www.southcoasttoday.com/article/19980220/news/302209955>.

¹⁴⁵ *Commonwealth v. Bly*, 862 N.E.2d 341, 351–52 (Mass. 2007) (discussing methods employed by Boston police to obtain suspect's DNA).

appear “racist”.¹⁴⁶ Additionally, experts testified that Bly’s DNA profile was found on clothes left behind on railroad tracks near the murder scene.

In his closing arguments, special prosecutor Thomas Brennan emphasized to a racially mixed jury of seven women and five men that Bly was the only person “on the planet” who had a motive to kill McLaughlin.¹⁴⁷ In spite of Bly’s defense lawyer’s argument that DNA testing was flawed and that gang associates were under intense pressure from Boston police to implicate Bly in the murder, the jury convicted Bly of first-degree murder Saturday in Suffolk Superior Court, ending a nearly four-year agonizing search for justice. Jeffrey Bly, who was 24 at the time, was immediately sentenced to life in prison without parole.¹⁴⁸

The court took a different approach toward handling the privacy issue in *Commonwealth v. Bly* where the suspect left behind a water bottle that he had brought with him to the police interview as well as cigarette butts after smoking; both were discarded at the police station after the interview.¹⁴⁹ In this case, the court did not assert Bly’s abandonment of those items as the reason for the lack of Fourth Amendment protection. Instead, the court’s decision was based on Bly’s “wholesale failure to manifest any expectation of privacy in the items whatsoever.”¹⁵⁰ In other words, it seems

¹⁴⁶ Ellement, “20 Years after His Murder,” at <https://www.bostonglobe.com/metro/2015/09/25/paul-mclaughlin-gang-prosecutor-murdered-west-roxbury-recalled-friends/RON4JgxWDo1GKfTxVca7FP/story.html>.

¹⁴⁷ Ellement, “20 Years after His Murder.”

¹⁴⁸ *Commonwealth v. Bly*, 862 N.E.2d 341. See also, Howland, “Inmate Charged in Prosecutor’s 1995 Murder,” at <https://www.southcoasttoday.com/article/19980220/news/302209955>.

¹⁴⁹ *Commonwealth v. Bly*, 862 N.E.2d 341, 349 n.3 (Mass. 2007). The defendant left the police station after an interview, leaving a water bottle and cigarette butts.

¹⁵⁰ *Commonwealth v. Bly*, 862 N.E.2d 341, 349 n.3 (Mass. 2007). 357.

that Bly neither adequately demonstrated ownership of the items, nor did he clearly show a lack of intent when he left behind his water bottle and cigarette butts at the police station.

State v. Reed

On March 10, 2003, Blake J. Reed was indicted for first-degree burglary, second-degree sexual offense, and common law robbery. On August 15, 2005, a jury found him guilty of first-degree burglary and second-degree sexual offense, but not guilty of common law robbery.

During the investigation, on January 28, 2003, two detectives from the Charlotte-Mecklenburg Police Department arrived at Reed's apartment to follow up with him as part of their investigation.

The two police officers interviewed Reed on a patio behind his apartment building. During the conversation, Reed lit a cigarette. After he finished smoking, Reed flicked the butt onto a pile of trash located in the corner of a concrete patio. The butt struck the pile of trash and rolled between Reed and one of the detectives who kicked the butt off the patio and on to the grassy common area. After the conversation ended, the detective retrieved the cigarette butt when his partner and Reed turned to go back inside the apartment.

After testing the retrieved cigarette butt, the State presented evidence that the DNA sample taken from the cigarette butt matched that taken from a stain found on the alleged victim's shirt. At trial, the defense moved to suppress this evidence on the grounds that it was the fruit of an unconstitutional search and seizure. The trial court

denied the defense's motion, and Reed was subsequently convicted. Thereafter, Reed appealed the order denying his motion to suppress.

Reed's sole argument on appeal was that the cigarette butt containing the DNA evidence was seized on the basis of a warrantless, non-consensual search of an area in which he had a reasonable expectation of privacy. The same Court of Appeals had recently held in *Rhodes* that "because the trash can was within the curtilage of [the] defendant's home and because the contents of the trash can were not placed there for collection in the usual and routine manner, [the] defendant maintained an objectively reasonable expectation of privacy in the contents of his trash can."¹⁵¹ The same analysis was applied in the Reed's case. More specifically, "in North Carolina, 'curtilage (an area of land attached to a house and forming one enclosure with it) of the home will be typically construed to include at least the yard around the dwelling house as well as the area occupied by barns, cribs, and other outbuildings.'" ¹⁵² Here, the patio was directly connected to Reed's apartment and covered from the apartment above by a tarp. Therefore, the cigarette fell within the curtilage of Reed's home, based on the North Carolina statute and the previous ruling in *State v. Frizzelle*.¹⁵³

By applying the ruling in *State v. Rhodes*, the North Carolina court ruled that Reed had a reasonable expectation of privacy, the search and seizure thus violated defendant's constitutional rights, and the trial court erred in denying the defendant's motion to suppress. The same North Carolina Court of Appeals had previously stated that

¹⁵¹ *State v Rhodes*, 151 N.C.App. at 215, 565 S.E.2d at 271.

¹⁵² 214, 565 S.E.2d at 270 and quoting *State v. Frizzelle*, 243 N.C. 49, 51, 89 S.E.2d 725, 726 (1955).

¹⁵³ 243 N. 243 N.C. 49, 51, 89 S.E.2d 725, 726 (1955).

“[t]he protection of the Fourth Amendment does not extend to abandoned property”¹⁵⁴ and “defendant could not have had any reasonable, legitimate expectation of privacy regarding the possession of said item after he discarded the same on a public street.”¹⁵⁵

The court granted that for abandonment to occur, the discarding of property must occur in a public place; one simply cannot abandon property within the curtilage of one’s own home.

Reed had a reasonable expectation of privacy in his home. The search and seizure as conducted by the police therefore violated Reed’s constitutional rights and the trial court’s denial of the defendant’s motion to suppress was in error. Accordingly, the North Carolina Court of Appeals reversed the trial court’s order and granted Reed a new trial.

Therefore, even in a case like *State of North Carolina v. Reed* in which the court suppressed prosecutorial evidence obtained from surreptitiously seized, out-of-body DNA, its analysis ultimately reflected an abandonment biased approach.¹⁵⁶ The court found that Reed had not abandoned the cigarette butt he had flicked onto his patio in the back of his apartment, an area for which the court found Reed had a reasonable expectation of privacy.¹⁵⁷

Commonwealth v. Cabral

In *Commonwealth v. Cabral*, the court found that the defendant had voluntarily abandoned the reasonable expectation of privacy he had in his saliva when he

¹⁵⁴ *State v. Cromartie*, 55 N.C.App 221, 225, 284 S.E.2d 728, 730 (1981).

¹⁵⁵ *Id.* at 223, 284 S.E.2d at 730.

¹⁵⁶ *State v. Reed*, 641 S.E.2d 320, 321–23 (N.C. Ct. App. 2007).

¹⁵⁷ *State v. Reed*, 641 S.E.2d 320, 321–23 (N.C. Ct. App. 2007).

“expectorated” on a public street.¹⁵⁸ The court held that the defendant’s expectoration in a public venue was a voluntary act and, therefore, he had abandoned all expectation of privacy he had in his saliva. With expectoration, the court found that “he assumed the risk of the public witnessing his action and thereafter taking possession of his bodily fluids.”¹⁵⁹

State vs. Christian

In May of 2003, Peter Christian was charged with burglary and third-degree sexual abuse based on allegations he entered Emily’s Iowa City apartment without her consent on October 26, 2002, and engaged in a nonconsensual sexual act with her.¹⁶⁰ During the 2004 jury trial, Emily testified that she went out drinking with her roommates at 11:00 p.m. that night. Around 2:30 a.m., Emily decided to leave the party on her own but informed her roommates. She recalled flagging down a taxicab to take her home. When Emily returned home, she left the door to the apartment unlocked. Emily spoke briefly with a friend on her cell phone and then reclined on a small couch to watch television. The next thing Emily remembered was being awakened by her roommates who were screaming, “Who was that guy?!”

Emily testified that she remembered everything “up until the time I fell asleep on the couch.” She denied consent to sexual contact with anyone or even knowing anyone had tried sexual contact with her. While trying to awaken Emily, her roommates observed

¹⁵⁸ *Commonwealth v. Cabral*, 866 N.E.2d 429, 433 (Mass. App. Ct. 2007).

¹⁵⁹ *Commonwealth v. Cabral*, 866 N.E.2d 429, 433 (Mass. App. Ct. 2007).

¹⁶⁰ *State v. Christian*, No. 04-0900, 2006 WL 2419031, at *1 (Iowa Ct. App. Aug. 23, 2006) (describing subterfuge employed by Iowa City police to collect suspect’s DNA).

that Emily's pants were undone and pulled down. They took Emily to the hospital to determine if she had been sexually assaulted. Emily was examined by an emergency room physician who collected specimens for a sexual assault kit. The examination did not reveal the presence of any sperm in Emily's vagina or cervix and the doctor was also unable to conclusively determine whether Emily's vagina had been penetrated. Iowa City police investigators subsequently sent Emily's sexual assault kit to the Iowa Department of Criminal Investigation (DCI) laboratory for DNA analysis. The DCI criminalist found a seminal stain on the inner crotch of Emily's underwear. Iowa City police considered Christian to be a suspect.

The Iowa City Rape Victim Advocacy Program (RVAP) informed police officer Jennifer Clarahan that they were interviewing Christian for a volunteer position on April 23, 2003. When Christian's RVAP interview was over, Officer Clarahan collected the water bottle and fork he had used during the interview and sent them to the DCI lab for analysis. The test results showed that the DNA on the water bottle and fork matched the DNA samples obtained from Emily's underwear. A subsequent search warrant application requested authority to detain Christian for collection of cheek swabs for additional DNA testing. These DNA tests confirmed the DNA samples already obtained from Christian matched those found in Emily's underwear.

Peter Christian testified to a different version of the evening's events. According to Christian, he and a friend were walking on the sidewalk when he saw Emily come out of her apartment building and cross the sidewalk in front of them. Christian did not see any cabs in the area. He observed Emily stumble on the curb as she turned around. Christian reached out his hand, said, "Are you okay?" and helped her up. Christian and

his friend talked with Emily, and she invited them up to her apartment where they watched television and continued to talk.

After Christian and Emily started to kiss, Christian's friend left and left Emily's apartment. Emily and Christian "continued to kiss and cuddle, it started to get to the stage of taking off clothes. I think she unzipped my pants and I ejaculated." Christian acknowledged Emily's pants were down, stated Emily did not appear to have been intoxicated, asserted the activities were consensual, and denied sexual intercourse or a sex act. Christian testified he continued to cuddle with Emily, and they fell asleep on the couch. Christian claimed he asked Emily's roommates to wake her up so Emily could explain "and they just grabbed my shirt and pushed me out the door."

The jury convicted Christian of third-degree sexual abuse and acquitted him of first-degree burglary. Christian appealed, and the Iowa State court affirmed his conviction. Christian was placed in the official sexual predator list as well.¹⁶¹

In *State v. Christian*, an undercover officer interviewing Christian for a volunteer position at the Iowa City Rape Victim Advocacy Program (RVAP) gave the suspect two water bottles, a slice of cake, and a fork during his interview with the city agency.¹⁶² When Christian left behind the used water bottles and fork, the court would not permit his Fourth Amendment constitutional expectation of privacy since those items had been abandoned like common trash.¹⁶³ Thus, the police could harvest Christian's DNA from the fork and water bottles, perform analysis, and provide results as evidence of innocence

¹⁶¹ *State v. Christian*, No. 04-0900, 2006 WL 2419031 (Iowa Ct. App. Aug. 23, 2006).

¹⁶² *State v. Christian*, 723 N.W.2d 453 (Iowa Ct. App. 2006).

¹⁶³ *State v. Christian*, 723 N.W.2d 453 (Iowa Ct. App. 2006).

or guilt. However, the court hinted at the possibility of a deeper, DNA-focused privacy analysis in its ruling, saying, “in the absence of any definitive authority to the contrary, we are unable to say Christian had a subjective or objective expectation of privacy in the DNA shed on the items seized.”¹⁶⁴ Subsequently, the court went on to note that Christian had abandoned any such expectation of privacy, even if it did exist.¹⁶⁵

State v. Athan

John Nicholas Athan, a former Seattle resident, was arrested twenty-one years after brutally killing his neighbor by strangulation and disposing of her body. The victim, Kristen Sumstad, was thirteen years old, and Athan was fourteen when he committed the crime and left her inside a cardboard box behind a television repair shop in Seattle’s Magnolia neighborhood where the teen lived. Although Athan was a suspect, not enough evidence was gathered and available to generate probable cause for a search warrant and pursue the case against him to seek justice for Kristen’s murder. Years passed, and Athan had moved to New Jersey where to start a new life. It was here where he received a letter that would ultimately lead to his capture and arrest.

Pretending to be a fictitious law firm, Seattle police sent a letter to Athan inviting him to join a class action lawsuit for overpaid parking tickets. After Athan licked a return envelope that the police had mailed to him, his DNA was extracted from the flap and tested for a match with that found on Kristen’s body. Athan’s DNA matched the sample that had been recovered from Sumstad’s body, and he was arrested, charged, and

¹⁶⁴ *State v. Christian*, 723 N.W.2d 453 (Iowa Ct. App. 2006).

¹⁶⁵ *State v. Christian*, 723 N.W.2d 453 (Iowa Ct. App. 2006).

convicted at trial.¹⁶⁶ When Athan's case went to trial, the DNA evidence collected by the police was the centerpiece.¹⁶⁷ The jury acquitted Athan of first-degree murder but convicted him of second-degree murder, twenty-nine years after he committed the crime.¹⁶⁸ He was sentenced to ten to twenty years under pre-sentencing reform act guidelines. Athan was considered a suspect from the beginning but there wasn't enough physical evidence to link him to the slaying for twenty years. He served about seven years behind bars after the parole board approved Athan's release from prison, stating in their report that he was "a low-risk for general and violent recidivism."¹⁶⁹

However, Athan's claim for a right to privacy of his body and bodily functions including saliva¹⁷⁰ was denied by the court. The court determined that, under the circumstances, Athan had "no inherent privacy interest in saliva."¹⁷¹ The court noted that Athan's saliva was neither obtained forcibly nor mandated as in cases like pre-employment urine analysis testing programs.¹⁷² They held the view that Athan had abandoned his saliva when he licked the envelope and mailed it, much like a situation when someone dumps garbage on a sidewalk, spits on a public street, or leaves cigarette

¹⁶⁶ Sullivan, "DNA on Envelope Sealed," at <https://www.seattletimes.com/seattle-news/dna-on-envelope-sealed-mans-conviction-in-82-murder-8212-now-hell-go-free/>, "John Nicholas Athan, the former Seattle man convicted of murder after he unwittingly gave police a DNA sample by licking an envelope, will be released on parole this year."

¹⁶⁷ Muenster, "DNA-case Ruses Damage," at http://old.seattletimes.com/html/opinion/2001849229_muenster03.html.

¹⁶⁸ *State of Washington v. John Nicholas Athan*, No. 75312-1 (2007), §8.

¹⁶⁹ Sullivan, "DNA on Envelope Sealed," at <https://www.seattletimes.com/seattle-news/dna-on-envelope-sealed-mans-conviction-in-82-murder-8212-now-hell-go-free/>.

¹⁷⁰ Sullivan, "DNA on Envelope Sealed," 33.

¹⁷¹ Sullivan, "DNA on Envelope Sealed," 33-34.

¹⁷² Sullivan, "DNA on Envelope Sealed," 33.

butts in a public ashtray.¹⁷³ Once mailed, the envelope—and subsequently his saliva—became police property,¹⁷⁴ and Athan had unwittingly relinquished all rights to its privacy.

As *amicus curiae*, the American Civil Liberties Union (ACLU) argued on Athan’s behalf that DNA “has the potential to reveal a vast amount of personal information, including medical conditions and familial relations,” and, thus, Athan was entitled to a privacy interest.¹⁷⁵ However, Washington State Supreme Court disagreed and stated,

While this may be true in some circumstances, the State’s use of Athan’s DNA here was narrowly limited to identification purposes. What was done with the letter, including DNA testing for the limited purpose of identification, was not within the sender’s control. The concerns raised by the ACLU, while valid, are not present in this case. The State used the sample for identification purposes only, not for purposes that raise the concerns advanced by the ACLU.¹⁷⁶

Maryland v. King

Alonzo Jay King Jr. was arrested for first- and second-degree assault. According to Maryland police protocol, the Maryland DNA Collection Act, a DNA sample was taken from King at the time of the arrest and entered into Maryland’s DNA database. The Act authorizes Maryland law enforcement authorities to collect DNA samples from “an individual who is charged with . . . a crime of violence or an attempt to commit a crime of violence; or . . . burglary or an attempt to commit burglary.”¹⁷⁷

¹⁷³ Sullivan, “DNA on Envelope Sealed,” 34.

¹⁷⁴ Sullivan, “DNA on Envelope Sealed.”

¹⁷⁵ Sullivan, “DNA on Envelope Sealed.”

¹⁷⁶ Sullivan, “DNA on Envelope Sealed.”

¹⁷⁷ See Sullivan, “DNA on Envelope Sealed,” 176; *Maryland v. King*, 569 U.S. 435 (2013).

DNA obtained from King matched a stain taken from an unsolved rape case in 2003. A Maryland officer presented the evidence to a Wicomico County grand jury, which called for an indictment and procured a warrant to obtain a second buccal DNA sample that could be used as incriminating evidence for the 2003 rape case.¹⁷⁸ King filed a motion to suppress the DNA evidence in the Circuit Court for Wicomico County stating that it infringed upon his Fourth Amendment rights, which prohibits unreasonable searches and seizures. His motion was denied, and King pleaded not guilty to the charge of rape and appealed the ruling. The Maryland Court of Appeals then reversed the original ruling, agreeing that the DNA sampling was a violation of the Fourth Amendment and could not be used as evidence. The State of Maryland appealed the Maryland Court of Appeals ruling and called for the case to be examined by the United States Supreme Court.¹⁷⁹

The decision was close, 5-4 in favor of Maryland. Justice Antonin Scalia, joined by Justices Ruth Bader Ginsburg, Sonia Sotomayor, and Elena Kagan, filed a scathing dissenting opinion. The justices maintained that “categorically” and “without exception,” “the Fourth Amendment forbids searching a person for evidence of a crime when there is no basis for believing the person is guilty of the crime or is in possession of incriminating evidence.”¹⁸⁰ The dissent also warned that “because of today's decision, your DNA can be taken and entered into a national database if you are ever arrested, rightly or wrongly,

¹⁷⁸ *Maryland v. King*, 569 U.S. 435 (2013).

¹⁷⁹ Schwinn, “Fourth Amendment,” Preview of United States Supreme Court Cases (2013): 215. American Bar Association.

¹⁸⁰ 133 S. Ct. at 1980.

and for whatever reason.”¹⁸¹ Justice Scalia took the rare step of reading his dissent from the bench, "signaling deep disagreement" on the Court.¹⁸²

The United States Supreme Court decided that “when officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.”¹⁸³

The majority concluded that it is reasonable for the law enforcement officers in the state of Maryland to conduct a minimally intrusive buccal swab of legitimately detained arrestees. The information obtained therein can then be used to determine whether the individual might be associated with a crime or even potentially a victim. This balances the state’s interests regarding detaining and charging arrestees and individuals’ interests regarding bodily integrity and informational privacy.

The significance of *Maryland v. King* is that it now places taking a DNA swab alongside fingerprinting as routine police booking procedure for arrested individuals. Those who support the decision believe it will help solve cold cases and future crimes. However, those against it will question whether the benefits of solving crime using this method will outweigh the privacy interests at stake.

¹⁸¹ 133 S. Ct. at 1999.

¹⁸² Liptak, “Justices Allow Police to Take,” at <https://www.kansas.com/news/article1116651.html>.

¹⁸³ *Maryland v. King*, 569 U.S. 435 (213).

Carpenter v. United States

Carpenter v. United States was a landmark United States Supreme Court case concerning the privacy of historical cellphone location records.¹⁸⁴ The Court held, in a 5–4 decision authored by Chief Justice Roberts, that the government violated the Fourth Amendment to the United States Constitution by accessing historical records containing the physical locations of cellphones without a search warrant. Some considered *Carpenter v. United States* to be “the most important Fourth Amendment case that the Supreme Court has heard in a generation.”¹⁸⁵

From December 2010 to March 2011, numerous RadioShack and T-Mobile stores in Michigan and Ohio were robbed by several men who entered the store wielding guns and demanding that store employees fill their bags with new smartphones. The robbers, who were from Detroit, Michigan, had conspired and participated in other armed robberies before. In April 2011, four of these smartphone robbers were apprehended and arrested, but Timothy Carpenter was not among them. When one of the arrested men confessed to the crime spree and turned over his phone, FBI agents could review the calls made from his phone around the time of the robberies.¹⁸⁶

In May and June 2011 and in compliance with the Stored Communications Act,¹⁸⁷ a magistrate judge granted the FBI’s request to obtain “transactional records” from

¹⁸⁴ *Carpenter v. United States*, 138 S. Ct. 2206; 201 L. Ed. 2d 507. Ng, “Supreme Court Says Warrant,” at <https://www.cnet.com/news/supreme-court-says-warrant-necessary-for-phone-location-data/>.

¹⁸⁵ Wessler, “The Supreme Court’s Most Consequential,” at <https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-most-consequential-ruling-privacy-digital>; Vladeck, “The Supreme Court Phone,” at https://www.vice.com/en_us/article/59zq5x/scotus-cell-location-privacy-op-ed.

¹⁸⁶ See *supra* note 182, *Carpenter v United States* 138 S. Ct. 2206; 201 L. Ed. 2d 507.

¹⁸⁷ The Electronic Communications Privacy Act of 1886 (P.L. 99-508). The Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses

various wireless carriers for sixteen different phone numbers for “all subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones . . . as well as cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls.”¹⁸⁸ The government was able to obtain a court order before gaining access to the information; prosecutors only had to show that they were seeking evidence relevant to a criminal investigation. Getting a search warrant requires the government to prove probable cause, which is cumbersome to obtain as it requires more specific information.¹⁸⁹

Although the sixteen different phone numbers recorded on the confessed robber’s cell phone around the time of the crime were not sufficient evidence to establish probable cause, it was enough under the Stored Communications Act. The Stored Communications Act requires only “that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.”¹⁹⁰ From the historical cell-site records that had been tracked for 127 days, the FBI were able to determine all of Carpenter’s cellphone locations and corroborate them with specific cell towers at the times of

voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).

¹⁸⁸ Brunner and Kohse, “Supreme Court Grants Cert,” at <https://www.lawfareblog.com/supreme-court-grants-cert-carpenter-v-united-states-overview>.

¹⁸⁹ Jehl et al., “Supreme Court Reenters Fray,” at <https://www.natlawreview.com/article/supreme-court-reenters-fray-privacy-carpenter-v-united-states>.

¹⁹⁰ Jehl et al., “Supreme Court Reenters Fray.”

robberies. From this information, the FBI ascertained that Carpenter was within a two-mile radius of four robberies.

Putting all pieces of information on Carpenter's whereabouts, cell phone calls, and location, the government charged and arrested Carpenter. A jury later convicted him on several counts of participating in a robbery that affected interstate commerce and another count of aiding and abetting the use or carriage of a firearm during a federal crime of violence. Carpenter was sentenced by Judge Sean Cox of the United States District Court for the Eastern District of Michigan to 1,395 months or 116.25 years in federal prison.¹⁹¹

Carpenter's case was reheard on appeal by the United States Court of Appeals for the Sixth Circuit, but the Court still sentenced him to 116 years in prison in June 2019. While Carpenter's lawyers argued that the cell phone tracking data should have been subject to the exclusionary rule¹⁹² and discarded as material collected without a proper warrant under the Supreme Court's ruling the judges believed that the FBI was acting in good faith with respect to collecting Carpenter's data based on the law at the time he committed his robberies.¹⁹³ Therefore, they upheld the trial court's admission of cellphone tracking locational evidence the FBI had surreptitiously gathered on Carpenter to be used as evidence during prosecutorial hearings. The Supreme Court had previously

¹⁹¹ *United States v. Carpenter*, 819 F. 3d 880, 885; Harris, "*Carpenter v. United States*: How Many."

¹⁹² Re, "The Due Process Exclusionary Rule," 1885. See also Alschuler, "Regarding Re's Revisionism," 302. The exclusionary rule is a legal rule based on constitutional law that prevents evidence collected or analyzed in violation of the defendant's constitutional rights from being used in a court of law.

¹⁹³ *Davis v. United States* (2011), 564 U.S. 229 (good-faith exception to the exclusionary rule).

ruled in 2011 that such good faith during his appeal as exemptions to the exclusionary rule are permissible in *Davis v. United States*.¹⁹⁴

In September 26, 2016, Carpenter petitioned the U.S. Supreme Court for a writ of certiorari.¹⁹⁵ On June 5, 2017, the U.S. Supreme Court agreed to review the case and consider whether the Fourth Amendment permits the government to collect cell phone records revealing an individual's location and movements over an extended period of time without first obtaining a warrant.¹⁹⁶ The Supreme Court heard Oral arguments on November 29, 2017,¹⁹⁷ with Nathan Freed Wessler, a staff attorney with the ACLU Speech, Privacy, and Technology Project representing Carpenter's interests.¹⁹⁸ Michael Dreeben, the Deputy Solicitor General in charge of the US Department of Justice argued on behalf of the United States.

On June 22, 2018, the Supreme Court of the United States issued its decision with a 5–4 split. Chief Justice John G. Roberts Jr. wrote for the majority with Associate Justices Ginsburg, Breyer, Sotomayor, and Kagan joining Roberts' opinion. "We decline to grant the state unrestricted access to a wireless carrier's database of physical location information Such exigencies," he wrote, "include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm or prevent the

¹⁹⁴ *Davis v. United States* (2011), 564 U.S. 229. See also Farias, "He Won a Landmark Case," at <https://www.nytimes.com/2019/06/13/opinion/timothy-carpenter-prison-privacy.html>.

¹⁹⁵ *Carpenter v. United States*, Docket Number 16-402, at <https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/>

¹⁹⁶ *Carpenter v. United States*, Docket Number 16-402.

¹⁹⁷ *Carpenter v. United States*, Docket Number 16-402.

¹⁹⁸ *Supra* note 185; Wessler, "The Supreme Court's Most Consequential."

imminent destruction of evidence.”¹⁹⁹ Furthermore, “the Constitution must take account of vast technological changes,” Chief Justice Roberts wrote, noting that digital data can provide a comprehensive, detailed—and intrusive—overview of private affairs that would have been impossible to imagine not long ago. The decision made exceptions for emergencies like bomb threats and child abductions. “Such exigencies,” he wrote, “include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm or prevent the imminent destruction of evidence.”²⁰⁰ Roberts also stressed that the decision is a very narrow ruling; it does not influence other parts of the third-party doctrine, such as banking records, nor does it prevent collection of cell tower data without a warrant in emergencies or for national security issues.²⁰¹

In his dissent, Justice Alito wrote,

I share the Court’s concern about the effect of new technology on personal privacy, but I fear that today’s decision will do far more harm than good. The Court’s reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.²⁰²

Justice Gorsuch’s dissent seems closer to a concurring opinion because he agreed with the majority’s decision while disagreeing with their reasoning. While Gorsuch concurred that law enforcement agencies need a warrant to obtain cell phone data, he disagreed that the Fourth Amendment provides the right to a “reasonable expectation of

¹⁹⁹ Liptak, “In Ruling on Cellphone Location,” at <https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html>.

²⁰⁰ Liptak, “In Ruling on Cellphone Location.”

²⁰¹ Totenburg, “In Major Privacy Win,” at <https://www.npr.org/2018/06/22/605007387/supreme-court-rules-police-need-warrant-to-get-location-information-from-cell-to>.

²⁰² *Carpenter v. United States*, Docket Number 16-402.

privacy.” Instead, Gorsuch argued that cell phone location records are the property of cell phone owners and under the Fourth Amendment, law enforcement agencies cannot search a person’s property without a warrant.²⁰³

In his dissent, Justice Neil Gorsuch seems to express disappointment that the third-party doctrine²⁰⁴ was not more broadly revisited. Although Gorsuch filed one of the four dissenting opinions, his dissent went further than the majority and read more like a concurrence on other grounds. The technical reason for Gorsuch deeming it a dissent was that Carpenter’s lawyers did not make the property-based argument Gorsuch favors. Rather than focus on the reasonable expectation of privacy analysis typically engaged in by the court in recent decades, Gorsuch’s dissent argues that the court should follow a property rights-based theory of the Fourth Amendment. Under that theory, Carpenter had a property interest in his cell phone data. Gorsuch’s decision to file a dissent may send a message to future defendants that without inclusion of a property-based argument his concurrence cannot be counted upon.

On remand from the Supreme Court, the United States Court of Appeals for the Sixth Circuit was required to reexamine whether the district court permitted the government to introduce Carpenter’s cell-site location information (CSLI) at trial, according to Fourth Amendment jurisprudence.²⁰⁵ The Court of Appeals explained that although the government should have obtained a warrant, it may affirm the district

²⁰³ *Carpenter v. United States*, Docket Number 16-402. See under Justice Gorsuch, dissenting.

²⁰⁴ Thompson, “The Fourth Amendment Third-Party Doctrine.” The third-party doctrine is a United States legal doctrine that holds that people who voluntarily give information to third parties—such as banks, phone companies, internet service providers (ISPs), and e-mail servers—have “no reasonable expectation of privacy.”

²⁰⁵ *Carpenter v. United States*.

court's decision if the government acquired Carpenter's CSLI in good faith reliance on the Stored Communications Act.²⁰⁶

The Sixth Circuit asked whether it was objectively reasonable for the government to rely on the statute at the time of the search and found that it was reasonable for the FBI agents to rely on the Stored Communications Act, under the circumstances.²⁰⁷ The court stated that the statute contemplates the Fourth Amendment's protections by specifying some instances where warrants are necessary, making it understandable why the agents believed a warrant was not required under certain circumstances when conducting a criminal investigation (Section 2703(d)). In Carpenter's case, the court stated that there is no evidence to indicate that the FBI agents who obtained the CSLI engaged in intentional misconduct. The court, therefore, affirmed the district court's decision; however, the court cautioned that going forward, the government must obtain a search warrant or rely on a recognized exception to the warrant requirement to obtain CSLI. The court also advised that to avoid "embarrass[ing] the future," courts must carefully and incrementally adapt their Fourth Amendment jurisprudence to advancements in the digital era.²⁰⁸

²⁰⁶ 18 U.S.C. Chapter 121 §§ 2701–2712). (The Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA)). §§ 2701–2712). (The Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party Internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA)).

²⁰⁷ FEDAgent, "On Remand from the Supreme Court," at <https://www.fedagent.com/columns/case-law-update/2856-on-remand-from-the-supreme-court-the-sixth-circuit-applies-the-good-faith-exception-in-carpenter>.

²⁰⁸ FEDAgent, "On Remand from the Supreme Court."

R. v. Stillman

*R. v. Stillman*²⁰⁹ was an important decision of the Supreme Court of Canada on Section 24(2) of the Constitution of Canada,²¹⁰ which allowed for the exclusion of evidence that is obtained in a manner that infringes the Charter, as it is commonly known.²¹¹ Section 24 of the *Canadian Charter of Rights and Freedoms* provides for remedies available to those whose *Charter* rights are shown to be violated. Some scholars have argued that it was actually section 24 that ensured that the *Charter* would not have the primary flaw of the 1960 *Canadian Bill of Rights*: namely, Canadian judges would be reassured that they could indeed strike down statutes on the basis that they contradicted a bill of rights.²¹² Following this case, the two-step Stillman test was developed for determining whether the admission of evidence obtained through a breach of a Charter right which would ultimately affect the fairness of this trial.²¹³

William Wayne Dale Stillman was 17 years old when he was arrested in 1991 for the brutal murder of a teenage girl in New Brunswick, Canada.²¹⁴ He was the last person seen with the victim on the night of the crime. He arrived home around midnight, cold, shaken, and wet from the upper thighs down with a cut above one eye and mud and

²⁰⁹ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

²¹⁰ Hogg, *Constitutional Law of Canada*, pp. 864-865.

²¹¹ Canadian Charter of Rights and Freedoms at <https://laws-lois.justice.gc.ca/eng/Const/page-15.html>.

²¹² Dyck, *Canadian Politics: Critical Approaches*, p. 442.

²¹³ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

²¹⁴ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

grass stains on his pants. He explained that he had been in a fight with five Indians but this explanation, as well as his account of where he had last seen the victim, varied over time.

The victim had died from wounds to the head. Semen was found in her vagina and a human bite mark had been left on her abdomen. At the police station, Stillman's lawyers informed the police by letter that he was not agreeable to provide any bodily samples, including hair and teeth imprints, or to give any statements; however, once Stillman's lawyers left, the police officers forcibly took his scalp hair and pubic hair samples as well as plasticine teeth impressions. Police officers subsequently interviewed Stillman for an hour in an attempt to obtain a statement.

After being permitted to call his lawyer, Stillman was escorted to the washroom by an officer. In the washroom, Stillman used a tissue to blow his nose. When he threw his mucous-containing tissue in the wastebasket, it was seized by a police officer and used for DNA testing. Stillman was arrested again, and a dentist took new impressions of the accused's teeth without his consent in a procedure lasting two hours. More hair was taken from Stillman along with saliva sample and buccal swabs.

Following *voir dire* (a preliminary examination of a witness or a juror by a judge or counsel which is held to determine the admissibility of certain evidence), the trial judge found that the hair samples, buccal swabs, and teeth impressions had been obtained in violation of section 8 of the Canadian Charter of Rights and Freedoms (the Charter) but concluded that the evidence was nevertheless admissible.²¹⁵ With respect to

²¹⁵ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

the tissue containing mucous, the trial judge found that it had not been obtained in violation of Section 8 and should thus be admitted.²¹⁶

Stillman was later convicted by a jury of first-degree murder. The majority of the Court of Appeal upheld the trial judge's ruling and affirmed the verdict. The court held (with L'Heureux-Dubé, Gonthier, and McLachlin dissenting) that the appeal should be allowed and a new trial ordered at which the hair samples, buccal swabs, and dental impressions should be excluded.

The Canadian Supreme Court found that the police had violated the law by taking Stillman's bodily samples and dental impressions, the procedures for which were considered highly intrusive.²¹⁷ As a minor, Stillman was entitled to the presence of an adult counsellor during police questioning. However, contrary to the specific instruction of his lawyers, the police interviewed Stillman at length and forcibly took bodily samples and dental impressions. This conduct was viewed as an "abusive exercise of raw physical authority" by the police.²¹⁸ Specifically, forcibly obtaining hair samples, buccal swabs, and dental impressions also infringed upon section 7 of the Charter²¹⁹ since it violated the right to security of the person in a manner that was considered inconsistent with the principles of fundamental justice. It was also described as the ultimate invasion of the accused's privacy and breached the sanctity of the body, which is essential to the maintenance of human dignity. Police actions taken without consent or authority that

²¹⁶ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

²¹⁷ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

²¹⁸ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

²¹⁹ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

intrude upon an individual's body in more than a minimal fashion violate, according to section 7 of the Charter.²²⁰

The *R v Stillman* case ultimately became a landmark decision of the Supreme Court of Canada on section 24(2) of the Constitution of Canada.²²¹ The Supreme Court decision allowed for the exclusion of evidence that is obtained in a manner that violates the *Charter*. Subsequent to the *Stillman* case, the two-step *Stillman* test was developed in conjunction with the earlier *Collins* Test²²² for determining whether the admission (or exclusion) of evidence that was obtained through a breach of a *Charter* right would affect the fairness of the trial.²²³ The issue of trial fairness comes into question when applying the first step of the *Collins* test²²⁴ to exclude evidence under section 24(2).²²⁵

Collins-Stillman Analysis

Under the *Collins* test, the administration of justice is brought into “disrepute” where a combination of three factors weight in favor of exclusion of evidence.²²⁶ These sets of factors consist of factors that

²²⁰ *R. v. Stillman*, 1 SCR 607, 1997 SCC 32.

²²¹ *R. v. Stillman*, 1 S.C.R. 607, 1997 SCC 32. *Note*: The case would later be replaced by the Supreme Court of Canada's decision in *R v Grant*.

²²² *R. v. Collins*, 1 S.C.R. 265, 1987.

²²³ *R v Grant* per McLachlin, C.J. and Charron, J., at paragraph 71.

²²⁴ See 236 *R. v. Collins*, 1 S.C.R. 265, 1987.

²²⁵ Dyck, *Canadian Politics: Critical Approaches*, p. 442. Section 24 of the *Canadian Charter of Rights and Freedoms* provides for remedies available to those whose *Charter* rights are shown to be violated. Some scholars have argued that it was actually section 24 that ensured that the *Charter* would not have the primary flaw of the 1960 *Canadian Bill of Rights*: Namely, Canadian judges would be reassured that they could indeed strike down statutes on the basis that they contradicted a bill of rights.

²²⁶ *R. v. Collins*, 1 S.C.R. 265, 1987.

1. affect the fairness of the trial,
2. are relevant to the seriousness of the violation; and
3. are relevant to the effect of excluding the evidence.

The Stillman test considers the first set of factors, namely the fairness of the trial. It examines the nature of the evidence and alternatives to its discovery.²²⁷ Therefore, the Stillman test compels the following analysis:

1. Classify the evidence as conscriptive²²⁸ or non-conscriptive²²⁹ based on the manner in which the evidence was obtained. If the evidence is non-conscriptive, its admission will not render the trial unfair and the Court will proceed to consider the seriousness of the breach and the effect of exclusion on the reputation of the administration of justice.²³⁰
2. If the evidence is conscriptive, and the Crown fails to demonstrate on a balance of probabilities that the evidence would have been discovered by alternative non-conscriptive means, its admission will render the trial unfair. As a general rule, the Court will exclude the evidence without considering the seriousness of the breach or the effect of exclusion on the reputation of the administration of justice.²³¹

²²⁷ *R. v. Stillman* (1997) 1 S.C.R. 607, 1997 SCC 32.

²²⁸ In other words, was the accused compelled to participate in the creation or discovery of the evidence?

²²⁹ Was the evidence “discoverable”? In other words, would the evidence have been discovered by an alternate non-conscriptive means?

²³⁰ Cheon-Hayes, “Stillman to Grant: When Form,” at http://www.cba.org/cba/cle/PDF/CRIM12_Paper_Cheon-Hayes.pdf.

²³¹ Cheon-Hayes, “Stillman to Grant: When Form.”

3. If the evidence is found to be conscriptive and the Crown demonstrates on a balance of probabilities that it would have been discovered by alternative non-conscriptive means, then its admission will generally not render the trial unfair. However, the seriousness of the Charter breach and the effect of exclusion on the repute of the administration of justice will have to be considered.²³²

Thus, the Stillman case led to a revision of the Canadian justice system with respect to collection of evidence to facilitate a fair trial and an impartial outcome.

Expectations of Privacy

It seems those U.S. courts that have analyzed the implications of Fourth Amendment on law enforcement's surreptitious harvesting of DNA and its subsequent analysis have also used a very narrow lens to arrive at their conclusion. Courts consider DNA contained in bodily fluid that is left behind, whether knowingly or unintentionally, or when it has not been taken using coercive methods, as no longer the private property of that individual. Courts have also decided on the issue of DNA privacy by remaining narrowly focused on the object upon which the DNA was found, articulating their opinion on a reasonable expectation of privacy test that was held in *Katz v. United States*. They used the abandonment analysis by applying the intrusion on place (body, in these cases) criteria as defined in the original Fourth Amendment text and by unequivocally stating that there was a lack of intrusion into the body. These reasons were used to further the argument that there was no reasonable expectation of privacy in all cases except *State*

²³² Cheon-Hayes, "Stillman to Grant: When Form."

of *North Carolina v. Reed*.²³³ Although the Supreme Court of Oregon hinted at the possibility of a reasonable expectation in *State v. Christian*,²³⁴ they did not grant Christian a reasonable expectation to privacy in the DNA he left behind in his fork and water bottles.

In *State v. Athan*,²³⁵ the Washington Supreme Court evaluated the situation narrowly by reiterating that the DNA was used solely for the purpose of identification by the police rather than the extremely private information that could be potentially revealed through analysis. The narrowness of the Washington Supreme Court's analyses of surreptitious harvesting demonstrate an antediluvian focus that could stem from a misapplication of *Katz v. United States* to situations that are presented in courts today. Contemporary cases centered on decisions regarding Fourth Amendment infringement involve genetic privacy cases where courts are presented with results from sophisticated forensic DNA technology, genealogy studies, and other genetic tests. While it may have seemed like an Orwellian fantasy at one time, advances in scientific innovation and technology today have made many things that were at one time unthinkable very possible today.

²³³ *State v. Reed*, 641 S.E.2d 320, 321–23 (N.C. Ct. App. 2007).

²³⁴ No. 04-0900, 2006 WL 2419031, at *1 (Iowa Ct. App. Aug. 23, 2006).

²³⁵ *State v. Athan* 158 P.3d 27, 32-34 (Wash. 2007).

Solving Cold Cases through STR Analysis

Golden State Killer Investigation (California)

Much has been written about the notorious Golden State Killer, and he has been the subject of numerous books, hundreds of articles, and a hit TV show on HLN that began airing in 2018. Also known by his other aliases, “East Area Rapist” and “Visalia Ransacker,” 72-year-old Joseph James DeAngelo was on the shortlist of suspects of the Bay Area police.²³⁶ They had been tracking him for decades, and as circumstantial evidence began building up against DeAngelo, the police would surreptitiously recover DNA samples that would ultimately connect him to the most notorious unsolved murder and rape spree in California.

Over the years, police had identified 8,000 possible suspects in the investigation. They began the meticulous task of eliminating each person through circumstantial evidence and were left with a list that included DeAngelo and a few others. “As the circumstantial evidence started to build up (against DeAngelo), we decided we needed to get his DNA,” said longtime cold case investigator Paul Holes. A career police detective, Holes has a special passion for solving cold cases and staying the course. Holes noted that investigators had recently begun using new DNA technology that both “allows the DNA to be a witness” and can potentially identify related suspects.

In DeAngelo’s case, detectives then gathered DeAngelo’s DNA from two places: some of it was taken from the handle of his car door, and some was taken from a discarded tissue in his trash.²³⁷ Investigators compared DNA from the killings for which

²³⁶ Gartrell, “Retired Cold Case Investigator.”

²³⁷ Hare and Taoushiani, “What We Know about,” at <https://www.cnn.com/2019/04/24/us/golden-state-killer-one-year-later/index.html>.

DeAngelo was a suspect to samples readily available to law enforcement, such as online ancestry databases. Through this process, investigators were able to identify a pool of people who were possibly related to the Golden State Killer. They meticulously searched genetic profiles on popular genealogy websites to see if they could find a DNA match to the murderer.²³⁸ Investigators were able to identify a genetic profile of someone who appeared to be related to the killer. Most of the investigation was conducted using an open-source genealogy website called GEDmatch, which provides genetic information for anyone to see—without a court order.

By this time, police had Joseph James DeAngelo under surveillance because they strongly suspected that he was the killer, but they needed more evidence than a possible familial DNA match. So, investigators simply waited for DeAngelo to discard something on which his DNA could be found. Law enforcement officials have not publicly divulged what those objects were, but they would have eventually obtained his DNA from something he left behind. With the help of modern DNA techniques and persistence, DeAngelo was arrested on April 24, 2018.

Prosecutors are unable to file charges in all cases of rape and burglary attributed to the East Area Rapist and Golden State Killer (also called the Visalia Ransacker and Original Night Stalker) because the statute of limitations has run out in those cases. As of now, the 72-year-old DeAngelo faces thirteen counts of murder with special circumstances, including murder committed during the course of a burglary and rape, as well as thirteen counts of kidnapping for robbery. He is charged in six different California counties—Sacramento, Santa Barbara, Orange, Ventura, Tulare, and Contra

²³⁸ Saplakoglu, “How the Golden State,” at <https://www.livescience.com/62421-golden-state-killer-dna-genealogy.html>.

Costa—and he will be tried on the multiple murder counts in a single trial in Sacramento. Prosecutors are seeking the death penalty in every county except Tulare and Contra Costa, for which the cases are not eligible for that sentence.²³⁹

Tracking Down BTK

Nola Foulston, the District Attorney in Wichita, Kansas, had spent almost two decades chasing the serial killer who called himself BTK, for “Bind, Torture, Kill.” When she started her pursuit in the 1970s, no one was using DNA evidence. But, by 2005, when Foulston felt she was closing in on the suspect, familial DNA connections were a key part of the crime fighter’s toolkit.²⁴⁰ Samples of the killer’s DNA from crime scenes were available to Foulston, and she had reason to believe that a man named Dennis Rader was BTK after computer discs sent to police were traced to a church computer to which only few, including Rader, had access. Foulston needed to confirm whether Rader’s DNA matched the killer’s that had been obtained from the crime scene, but police decided not to simply ask Rader to provide a sample of something that would have his DNA. Foulston is quoted as having said, “They didn't have everything they needed at that point to take him into custody, so you'd be leaving a guy out there with his DNA sample hanging out. And he was not inactive. He continued to plan homicides up until the day that we caught him.”

The investigative team learned that Rader’s daughter had recently had medical testing. Under a judge's court order, investigators obtained access to a sample of the

²³⁹ Hare and Taoushiani, “What We Know about,” at <https://www.cnn.com/2019/04/24/us/golden-state-killer-one-year-later/index.html>.

²⁴⁰ Shapiro, “Police Use DNA to Track,” at <https://www.npr.org/templates/story/story.php?storyId=17130501>

daughter's DNA from the hospital. In 24 hours, when the STR results came back, the police found that it was a familial match (i.e., the daughter's hospital DNA result was consistent with her being the biological child of the owner of the crime scene DNA). Police then arrested Dennis Rader and brought him to a special facility for interrogation. This conversation followed:

One of the officers asked Rader, "You know why you're here?"

Rader replied, "I assume it's about BTK."

The officer asked, "Would you be surprised to know that the father of your daughter is BTK?"²⁴¹

Foulston noted that stunned silence followed. Then, "The FBI agent said, 'Tell us who you are.' And he said, 'I'm BTK. You got me.'"

Dennis Rader was arrested while driving near his home in Park City, Kansas shortly after noon on February 25, 2005.²⁴² Following his arrest, Rader was charged with 10 counts of first degree murder on February 28, 2005.²⁴³ On March 1, Rader's bail was set at US\$10 million, and a public defender was appointed to represent him.²⁴⁴ Then on March 5, news outlets claimed to have verified by multiple sources that Rader had

²⁴¹ Shapiro, "Police Use DNA to Track Suspects through Family."

²⁴² "'BTK' Serial Killer in Custody, Claims Police," *St. Petersburg Times*, March 1, 2005, https://web.archive.org/web/20080409111913/http://www.sptimes.ru/index.php?action_id=2&story_id=2857; Hansen, "How the Cops Caught BTK," *ABA Journal*, May 1, 2006, http://www.abajournal.com/magazine/article/how_the_cops_caught_btk.

²⁴³ "'B.T.K.' Suspect Charged," *New York Times*, March 1, 2005, <https://www.nytimes.com/2005/03/01/national/btk-suspect-charged-with-10-murder-counts.html>. See also "BTK Sentenced to 10 Life Terms," *CNN*, August 18, 2005, <http://www.cnn.com/2005/LAW/08/18/btk.killings/>.

²⁴⁴ See *supra* note 238 and "Victim's Brother Describes Killing," *CNN*, March 2, 2005, <http://www.cnn.com/2005/LAW/03/02/btk.investigation/>.

confessed to the ten murders he was charged with, but no others.²⁴⁵ On May 3, the judge entered not-guilty pleas on Rader's behalf as Rader did not speak at his arraignment.²⁴⁶

However, on June 27, the scheduled trial date, Rader changed his plea to guilty. He described the murders in detail, making no apologies for his crime.²⁴⁷

On August 18 Radar was sentenced to ten consecutive life sentences with a minimum of 175 years to serve.²⁴⁸ Kansas had no death penalty at the time of the murders.²⁴⁹ In 2006, due to good behavior, Rader was allowed access to television and radio, to read magazines.²⁵⁰ Rader is now in solitary confinement for his protection with an hour of exercise per day and showers three times per week. These privileges are likely to continue indefinitely and until his death in prison.

Popular DJ Caught after 26 Years

Due to the dedicated effort of Lancaster County, Pennsylvania, District Attorney Craig Stedman, his team members, and Parabon NanoLabs, a Reston, Virginia-based company, Raymond Charles Rowe was arraigned for the rape and murder of a beloved

²⁴⁵ “Rader Has Admitted to Killings,” *DeseretNews*, March 6, 2005, <https://www.deseret.com/2005/3/6/19880643/rader-has-admitted-to-killings-daily-says>.

²⁴⁶ Strongin and Hurst, “Families of BTK Victims,” *Wichita Eagle*, May 5, 2005, <https://www.kansas.com/news/special-reports/btk/article1003691.html>.

²⁴⁷ “Anger, Relief over BTK Confessions,” CBS News, June 28, 2005, <https://www.cbsnews.com/news/anger-relief-over-btk-confessions/>; Hansen, “How the Cops Caught BTK”; Sales, “US Serial Killer Pleads Guilty to Ten Murders,” *World Today*, June 28, 2005, <http://www.abc.net.au/worldtoday/content/2005/s1402337.htm>.

²⁴⁸ Hickey, *Serial Murderers and Their Victims* (Cengage Learning, 2013), 254.

²⁴⁹ “BTK Sentenced to 10 Life Terms.”

²⁵⁰ “Who is Dennis Rader aka the BTK Serial Killer?” *Wichita Eagle*, updated August 12, 2019, <https://www.kansas.com/news/special-reports/btk/article225082655.html>; Sylvester, “Investigators tell of grisly crimes, Rader's delight,” in Simpson, *The Serial Killer Files* (Chapter 25), The Little Brown Book Group (2017).

school teacher, Christy Mirack, at her East Lampeter Township home twenty-six years after the crime.²⁵¹ Stedman credited Parabon NanoLabs with providing the critical analysis that allowed the DA's office to file the charge.

A well-known disc jockey living in plain sight only a few miles from the alleged brutal rape and homicide, Rowe left a used water bottle and gum after working at an elementary school event. From these two pieces of evidence, the police recovered his DNA. Meanwhile, the DNA obtained from the scene of the crime had been sent to a laboratory, which created "a DNA phenotype 'composite' of the killer's attributes," including the color of hair, eyes, and skin.

CeCe Moore, the lead genealogist for Parabon NanoLabs, a small DNA technology company that is leading the way in genetic genealogy said that when she received the genetic information for Mirack's killer, she determined the suspect had half Northern European ancestry from his mother's side. She could also predict that the suspect was half Puerto Rican, both from Parabon's phenotyping estimation and from his relatives who shared his DNA in the genealogy database.²⁵² "And then, online there was an article that he had been interviewed for as kind of a minor celebrity. And he said he liked cooking Puerto Rican food because he was half Puerto Rican. And that was it. That

²⁵¹ Shapiro, "DNA on Gum, Water," ABC News, June 26, 2018, <https://abcnews.go.com/US/dna-gum-water-bottle-leads-djs-arrest-26/story?id=56165384>.

²⁵² Farmer, "Using Genetic Genealogy to Convict," CBS News, January 9, 2019, <https://www.cbsnews.com/news/dj-freez-pleads-guilty-using-genetic-genealogy-to-convict-raymond-charles-rowe-60-minutes/>.

was the final piece of evidence I needed,” said Moore.²⁵³ According to prosecutors, the phenotype report was released to the public in November 2017.²⁵⁴

“The phenotype report included visual composites of what the killer would look like at various ages,” prosecutors said. “That data and associated composites were released to the public in November 2017.”²⁵⁵ The genealogy firm, Parabon Nanolabs, phenotyped DNA evidence from the crime scene and released three composite sketches of what Rowe could be predicted to look like at age 25, 45, and 55.²⁵⁶ A sketch released by Lancaster, PA online newspaper predicted eye color, eyebrow shape, hair color and jawline shape accurately.²⁵⁷

The Mirack case had hindered investigators until authorities working with DNA from the crime scene used a publicly available genealogical database to identify a half-sister of the then-unknown suspect.²⁵⁸ The half-sister’s whereabouts led them to Rowe, who had lived just miles from where the killing occurred. The combination of predicted phenotype from DNA analysis, the published interview with Rowe asserting his ethnic background, and personal preferences all led to piecing the parts of the puzzle that had long eluded investigators. Thus, the information within DNA can function as a sleuth and

²⁵³ Farmer, “Using Genetic Genealogy to Convict.”

²⁵⁴ Shapiro, “DNA on Gum, Water,” at <https://abcnews.go.com/US/dna-gum-water-bottle-leads-djs-arrest-26/story?id=56165384>.

²⁵⁵ *Supra* note 181; Shapiro, “DNA on Gum, Water.”

²⁵⁶ Schweigert, “Raymond Rowe, the Ex-DJ,” at <https://fox43.com/2018/07/23/raymond-rowe-the-ex-dj-accused-in-christy-mirack-murder-case-waives-preliminary-hearing/>.

²⁵⁷ Hawkes and Knapp, “Raymond ‘DJ Freez’ Rowe Arrested,” *Lancaster Online*, June 25, 2018, https://lancasteronline.com/news/local/raymond-dj-freez-rowe-arrested-for-killing-of-schoolteacher-christy/article_f05a2ee4-78b2-11e8-ad10-4382ef42f96d.html5.

²⁵⁸ “DJ Pleads Guilty,” *Guardian*, January 8, 2019, <https://www.theguardian.com/us-news/2019/jan/08/pennsylvania-dj-dna-schoolteacher-murder>.

solve crime after several years have passed, bringing an end to the cold case and closure to those left behind.

With DNA evidence linking him to the crime scene, Raymond Rowe pled guilty to the murder of Christy Mirack in 1992.²⁵⁹ The plea deal saved Rowe from the death penalty. Craig Stedman, the Lancaster County District Attorney, said that investigators could not prove a direct connection between Rowe and Mirack although the two of them frequented the same social clubs. Stedman said Rowe did not provide a motive but that Rowe's route to work took him past Mirack's apartment complex. According to prosecutors, Rowe drove a white Toyota Celica in 1992, which matched the vehicle that witnesses saw parked in odd places at the complex on the morning of the murder. "He's a rapist. He's a murderer, and he took her life, and he's going to spend the rest of his days behind prison," said Stedman.

Reasonable Expectations of Privacy in Discarded Items

In the landmark U.S. cases examined so far, the majority of the courts have avoided the question of whether the defendant had any reasonable expectation of privacy in the discarded cells recovered from their saliva or blood including the DNA contained within those cell walls.²⁶⁰ Instead, the courts questioned if there was a reasonable expectation of privacy in discarded items, such as the water bottle, drinking cup, straw (*Sigsbee*), or fork (*Christian*). It would have been just as appropriate question in *Katz* to

²⁵⁹ "Raymond 'DJ Freeze' Rowe Pleads Guilty," at <https://www.wgal.com/article/hearing-scheduled-for-raymond-dj-freeze-rowe-accused-killer-of-christy-mirack/25780588>.

²⁶⁰ The *Athan* and *Sigsbee* courts briefly asked some versions of the question and concluded in the negative without any substantial analysis. *State v. Athan*, 158 P.3d at 33; *People v. Sigsbee*, No. 03-0342, slip op. at 31–33 (Onondaga, N.Y. Cnty. Ct. Oct. 30, 2003).

consider whether he had a reasonable expectation to privacy in certain private phone communications. Writing for the majority in *Katz*, Justice Stewart wrote, “One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.”²⁶¹ So, too, in surreptitious harvesting cases, the question of whether reasonable expectation of privacy in out of body DNA must be addressed. Additionally, courts should address the sensitivity of personal information that DNA encodes from color of eyes, propensity for certain illnesses to lifestyle preferences.

We may not expect privacy, but, surprisingly, most people think posting on social media is not unsafe. Facebook users can choose from a drop-down menu whether they want their posts to be seen by the public, just friends, or just by the user alone. Users are (or should be) aware of this option. However, in spite of promises to keep users’ personal information confidential, it was leaked recently or “compromised,” as Facebook called it. Millions of people were affected, and Mark Zuckerberg was asked to testify in front of Congress and address this breach of privacy. While Facebook claims that they are innocent, that has yet to be proven. All social media channels make their income through advertising and clandestinely selling personal information of their users. We can delete posts, too, but are they really gone forever or held in some part of cyberspace that most do not know about and never access?

Ostensibly, courts have not fully developed the Fourth Amendment analysis in its application to surreptitious DNA harvesting and analysis. Rather, DNA analysis has been

²⁶¹ *Katz v. United States*, 389 U.S. 347, 361 (1967).

compared to fingerprint analysis, a technique that is routinely used to identify and connect a suspect to the scene of a crime. In such comparisons, genetic privacy is either viewed through the prism of property, a physical location (oftentimes, the body), or a piece of information.

In the property model, discarded DNA is considered abandoned and is, therefore, no longer attached to the owner. In this scenario, a person's DNA becomes public property on a first-come, first-served basis. In the physical location model, either the separated DNA is no longer part of the person's body, and whoever takes it for analysis is not physically intruding into the body, or both. In the information model, law enforcement officials are gathering DNA just as they would when dusting a crime scene for fingerprints. In this case, the courts state that subsequent DNA analysis is used to identify potential crime suspects just as fingerprinting has been utilized in traditional investigative procedures.

Courts that conducted an intrusion on property analysis asked whether the defendant had a reasonable expectation of privacy in the discarded items. None of these courts asked whether the defendant had a reasonable expectation of privacy in his out-of-body DNA or in his cells that contained DNA. Just as the appropriate question in *Katz* was whether Katz had a reasonable expectation of privacy when communicating by phone in a booth, a similar question can be posed in the surreptitious harvesting of discarded DNA. Here, the appropriate question is whether the defendants had a reasonable expectation to privacy in their out-of-body DNA and the personal sense of privacy that is attached to their genetic material.

Thus, information gathered is both non-intrusive and unidimensional with a singular purpose of identification, according to the courts' analyses.²⁶² Under these analytical paradigms, courts find that no Fourth Amendment reasonable expectation of privacy has been violated when discarded or abandoned DNA is surreptitiously harvested. Those who have studied these possible scenarios have accepted that these types of court cases will result in similar rulings that can be expected to continue for the foreseeable future.²⁶³

The *Katz*, *Kyllo*, and *Jones* cases²⁶⁴ have ruled on the Fourth Amendment by extending beyond traditional boundaries of a house, body, and papers. The implication that the intruded property be physically attached to qualify for a reasonable expectation of privacy was tested in each of these cases. In each case, the Supreme Court ruled that the intrusion by the government was a Fourth Amendment search where a court-ordered search warrant was a prerequisite. In the *Katz* case, a listening device was attached outside a public phone booth. In the *Kyllo* case, the government was measuring heat emanating from a house as it was escaping into the atmosphere. In the *Jones* case, a GPS tracking device was attached to Jones' car to investigate his whereabouts. All three cases were intrusions conducted outside the home and did not directly involve body or papers.

²⁶² The *Athan* and *Sigsbee* courts briefly asked versions of the question and concluded in the negative without any substantial analysis. *Athan*, 158 P.3d at 33; *People v. Sigsbee*, No. 03-0342, slip op. at 31–33 (Onondaga, N.Y. Cnty. Ct. Oct. 30, 2003).

²⁶³ Joh, "Reclaiming 'Abandoned' DNA," *supra* note 55, 857, 882 (suggesting that DNA is different and argues that the idea of genetic exceptionalism suggests that we should be more cautious in using preexisting analogies to capture the full import of a new technology). See also Kaye, "Science Fiction and Shed DNA," *supra* note 51, 420. And, Kaye, "The Science of DNA Identification," 409, 420.

²⁶⁴ *Katz v. United States*, 389 U.S. 347, 361 (1967); *Kyllo v. United States*, 533 U.S. 27, 29–30 (2001); *United States v. Jones*, 132 S. Ct. 945, 951 (2012).

Consequently, the Court was asked to test the idea of a type of privacy that was intangible and had to do with personal space, rather than a direct invasion of property.

The depth, nature, and scope of protection that the Fourth Amendment ensures safeguarding personal privacy may not be apparent from the original text. It guarantees that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated....” At first glance, it is somewhat obvious that security from intrusions on a person’s physical privacy is guaranteed by the Constitution. Physical privacy can be interpreted to be property, the body, and physical items that constitute tangible ownership in the traditional concept of privacy.

While the Fourth Amendment says nothing about an individual’s right to privacy and security from intrusions involving modern gadgets, like a GPS device,²⁶⁵ hidden cameras, eavesdropping mechanisms, or heat measuring devices,²⁶⁶ courts have ruled on such matters. Neither does the Fourth Amendment make any reference to privacy guaranteed for items discarded from the body, including bodily fluids that contain cells and, within them, DNA. Each of these intrusions is a tangible piece of property or place. Technical developments that could subsequently be used for personal intrusion had not been conceptualized by the Framers when the Constitution was written; however, they are realities of contemporary society and, therefore, must be addressed in the debate of what constitutes privacy in a modern context.

²⁶⁵ *Carpenter v. United States*, Docket Number 16-402.

²⁶⁶ *Kyllo v. United States*, 533 U.S. 27, 29–30 (2001).

A case that illustrates the fragility of the ownership of cellular matter is addressed in *Moore v. Regents of the University of California*, a landmark Supreme Court of California decision involving a civil action over the property rights to one's own cells taken as samples by doctors or researchers.²⁶⁷ John Moore was treated by physician and researcher David Golde at the University of California Los Angeles (UCLA) Medical Center for hairy-cell leukemia. The course of treatment from October 1976 to September 1983 included several visits where Dr. Golde removed blood, bone marrow aspirate, and several other bodily substances from Moore. When Moore wanted to transfer his care to his new home in another state, Golde offered to cover the expense of Moore's airfare and accommodations in Los Angeles, and Moore agreed to continue his patient care with Golde.²⁶⁸

In August of 1979, Golde established a "cell line" from spleen cell matter taken from Moore's body due to their interesting property. Moore's blood cells were unique in that they produced a protein that stimulated the growth of white blood cells, which help to protect the body from infections.²⁶⁹ Thereafter, on January 30, 1981, the Regents of University of California applied for a patent on the cell line, presumably to benefit monetarily from Moore's cells, which were originally taken as samples and subsequently immortalized for commercial purposes with the help of biopharmaceutical companies. Golde and his research assistant, not Moore, were named as beneficiaries of any

²⁶⁷ *Moore v. Regents of the University of California*, 793 P.2d 479 at 490 (Cal. 1990).

²⁶⁸ Skloot, "Taking the Least of You," at <https://www.nytimes.com/2006/04/16/magazine/taking-the-least-of-you.html>.

²⁶⁹ McLellan, "John Moore, 56; Sued to Share," at <https://www.latimes.com/archives/la-xpm-2001-oct-13-me-56770-story.html>.

monetary gain that would accompany this commercialization.²⁷⁰ On March 20, 1984, a patent was issued and named Golde and Quan, another researcher at UCLA, as the inventors and the Regents of the University of California as the assignee. Biotech firms Genetics Institute Inc., and Sandoz Pharmaceuticals were also added to *Moore v. Regents of the University of California* due to their subsequent investments in the cell line. Moore brought suit on July 9, 1990, alleging conversion of his bodily fluids had occurred by UCLA.²⁷¹

On the question of whether John Moore retained an ownership interest in his own excised cells and cellular matter such that he may sue David Golde and UCLA for profiting from a commercial cell line created from his cells, the California Supreme Court held that Moore did not have that right. However, the Court granted that Moore may have the right to sue for claims based on “breach of fiduciary duty and lack of informed consent.”²⁷² The majority opinion first examined Moore’s claim of property interests under existing California law. The court first rejected the argument that a person has an absolute right to the unique products of their body, as his products were not unique and the cells are “no more unique to Moore than the number of vertebrae in the spine or the chemical formula of hemoglobin.”²⁷³ Justice Arabian wrote a concurring opinion, asserting that the deep philosophical, moral, and religious issues presented by the case could not be decided by the court. However, Justice Mosk dissented, stating that Moore could have been denied some property rights and given others. At the very least, Moore

²⁷⁰ McLellan, “John Moore, 56; Sued to Share.”

²⁷¹ *Moore v. Regents of the University of California*, 793 P.2d 479 at 490 (Cal. 1990).

²⁷² *Moore v. Regents of the University of California*, 793 P.2d 479 at 490 (Cal. 1990).

²⁷³ *Moore v. Regents of the University of California*, 793 P.2d 479 at 490 (Cal. 1990).

had the “right to do with his own tissue what the defendants did with it.” In an article published by the newspaper, the *Los Angeles Times*, “Moore later negotiated what he called a 'token' settlement with UCLA that covered his legal fees based on the fact that he wasn't informed and hadn't agreed to the research.”²⁷⁴

More recently, the issue of guardianship of HeLa, a well-known cell line named after Henrietta Lacks that has been in existence since 1951, has come to fore.²⁷⁵ Christina J. Bostick, a lawyer representing the eldest son and two grandsons of Henrietta Lacks, whose “immortal cells” named HeLa have been the subject of a best-selling book, a TV movie, a family feud, cutting-edge medical research, and a multibillion-dollar biotech industry, announced that she plans to file a petition seeking “guardianship” of the cells on behalf of Lawrence Lacks, the eldest son of Lacks, and grandsons Lawrence Lacks, Jr., and Ron Lacks.

The original cells from the now well-known and established cell line were taken without consent from Lacks, an African American, during a 1951 visit to Johns Hopkins Hospital in Baltimore, which was racially segregated at the time. When she went to Johns Hopkins Hospital for bleeding, doctors discovered a malignant tumor on her cervix and subsequently collected cells from the tumor without her knowledge or consent, according to a report by Johns Hopkins Medicine.²⁷⁶ To their astonishment, scientists at Johns Hopkins discovered that unlike the cells they had collected from other sources, which

²⁷⁴ McLellan, “John Moore, 56; Sued to Share.”

²⁷⁵ DeNeen L. Brown, “Can the ‘Immortal Cells’,” at <https://www.washingtonpost.com/news/retropolis/wp/2018/06/25/can-the-immortal-cells-of-henrietta-lacks-sue-for-their-own-rights/>.

²⁷⁶ John Hopkins Medicine, “The Legacy of Henrietta Lacks,” at <https://www.hopkinsmedicine.org/henrietalacks/index.html>.

ceased to grow almost immediately outside the human body, Lacks's cells not only thrived, but in fact, doubled every twenty to twenty-four hours.²⁷⁷

Although Lacks died on October 4, 1951, her cells continued to live beyond her thirty-one years of age. "HeLa" cells, which were named after the first two letters of Lacks's first and last names, would go on to contribute towards significant advances in scientific research leading to two Nobel Prizes in research, the development of vaccines, cancer treatments, *in vitro* fertilization, and a genome sequence that was published last year.²⁷⁸ The cells have been used in the research of toxins, hormones, and viruses and to study the effects of radiation and the development of the polio vaccine. "There are 17,000 U.S. patents that involve HeLa cells, which are theoretically continuing to make money," said Bostick.²⁷⁹

Since the statute of limitations for medical malpractice expired many years ago and today, the question of ownership remains complicated. Although Johns Hopkins has no claims to the cell line "because the cells cannot be patented," Bostick said that she will use "creative litigation" to help the Lacks family members regain some kind of control of their mother's cells, which have been reproduced billions of times for medical research. Bostick's strategy in resolving guardianship can be one of several, including

saying Henrietta Lacks is a person who is continuing to be represented in life by her cells, or that Henrietta's cells themselves are Henrietta Lacks and in so doing she is still living, or her cells are the property of the estate

²⁷⁷ John Hopkins Medicine, "The Legacy of Henrietta Lacks."

²⁷⁸ Racaniello, "Henrietta Lacks (HeLa) Genome Sequence," at <http://www.virology.ws/2013/03/27/henrietta-lacks-hela-genome-sequence-published-then-withdrawn/>.

²⁷⁹ Brown, "Can the 'Immortal Cells'," at <https://www.washingtonpost.com/news/retropolis/wp/2018/06/25/can-the-immortal-cells-of-henrietta-lacks-sue-for-their-own-rights/>.

because they belong to her and require protection because she is now deceased and cannot speak on her behalf for her property.²⁸⁰

Historical Views on Property and Place

Historically, the U.S. Supreme Court's Fourth Amendment jurisprudence reflected a rigid and relatively narrow legalistic focus on property and place in defining the extent of its protection of privacy.²⁸¹ A physical invasion or a search of a person, papers, or tangible material effects, constituted a Fourth Amendment search, and outside those areas, a violation and, by extension, a reasonable expectation of privacy was not possible.²⁸² In this narrow framework, privacy referred to the concept of property rights and little more.²⁸³

Katz v. United States

In 1967, *Katz v. United States* was presented to the Supreme Court.²⁸⁴ In its ruling, albeit in a narrow five to four split decision, the Court abandoned its traditional models of property and place as exclusive standards for determining whether a violation of Fourth Amendment privacy by the government had taken place. To eavesdrop on Katz, who was suspected of engaging in illegal gambling across Florida, Massachusetts, and California, the government attached a listening and recording device outside a telephone

²⁸⁰ John Hopkins Medicine, "The Legacy of Henrietta Lacks," at <https://www.hopkinsmedicine.org/henriettalacks/index.html>.

²⁸¹ See, for example, *Olmstead v. United States*, 277 U.S. 438, 464 (1928) ("The Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects.").

²⁸² *Olmstead v. United States*, 277 U.S. 438, 464 (1928), 466.

²⁸³ Simmons, "From Katz to Kyllo," 1308-1309.

²⁸⁴ *Katz v. United States*, 389 U.S. 347 (1967).

booth that Katz frequently used to make phone calls.²⁸⁵ Subsequently, the evidence gathered by the FBI was used to convict Katz of illegal gambling activities.²⁸⁶

The government had not invaded Katz's home or body or even entered the telephone booth. Technically, there were no intrusions on Katz's property or entry inside the phone booth that he used for making telephone calls. Katz was initially convicted based on the recordings that the FBI collected as evidence in his gambling activities. He challenged the conviction, arguing that the recordings were obtained in violation of his Fourth Amendment rights. The United States Court of Appeals, Ninth Circuit based in San Francisco, CA, sided with the FBI because there was no physical intrusion into the phone booth itself; however, the case reached the higher judicial authority, the U.S. Supreme Court.²⁸⁷

In its decision, the Supreme Court redefined its approach to the Fourth Amendment privacy by shifting the question away from the narrow, technical legal status of person and place. Instead, the Court examined whether Katz had a reasonable expectation of privacy within a given radius from the phone booth and if this area of personal privacy had been violated by the government. The Court also defined an updated version of the measurement of privacy at that was stake. In his concurrence, Justice Harlan wrote,

For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection... But what he seeks to preserve

²⁸⁵ *Katz v. United States*, 389 U.S. 347 (1967), 348, 354.

²⁸⁶ *Katz v. United States*, 389 U.S. 347 (1967), 348.

²⁸⁷ *Katz v. United States*, 389 U.S. 347 (1967), 361.

as private, even in an area accessible to the public, may be constitutionally protected.²⁸⁸

The Court was suggesting that Katz demonstrated through his actions, and from his body language, that he expected privacy while engaged in a telephone conversation in the closed booth. Therefore, Katz had a Fourth Amendment privacy interest into which the government intruded even if it did so in a space that is technically public and was neither rented nor owned by Katz. Thus, in its ruling of the Katz case, the Supreme Court set a precedent for an innovative concept of privacy that was novel and had not been addressed until then.

The use of “people, not places” by the Court also suggests that the notion of privacy was expanded to include a more intangible interest than the one residing within the space of an enclosed telephone booth. Katz chose a phone booth, entered that space, and closed the door behind him, expecting to have a private conversation and not just enter a private space.²⁸⁹ Therefore, the use of “people” in the Court’s words referred to Katz’s attitude towards the conversation and its content, seeking to keep them private through his behavior. Both Katz’s behavior and the information that he wanted to protect from outsiders indicated to the Court that he felt a sense of privacy. The technical, property-based approach had traditionally been the court’s interpretation of privacy. But, the shift in focus to a more intangible and personal concept of privacy opened the door

²⁸⁸ *Katz v. United States*, 389 U.S. 347 (1967), 351-352.

²⁸⁹ *Katz v. United States*, 389 U.S. 347 (1967).

not only to another notion of privacy, but also an increase to the scope of its definition and the yardstick by which to measure this new concept of personal privacy.²⁹⁰

Justice Harlan's concurrence described how to assess the nature and scope of any possible Fourth Amendment privacy interest a person might hold. He wrote, "there is a twofold requirement, first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Thus, Justice Harlan's "twofold requirement" for measuring whether privacy interest is at stake warrants the protection of the Fourth Amendment: the Katz test. It also expanded the question of privacy. Most importantly, it placed the issue of privacy in the context of the case and asked whether privacy was protected according to the Fourth Amendment under a specific set of circumstances.

It seems that the Court offered little guidance on how to go about this process other than how to solve the case based on the circumstances of Katz's case. A single ungrounded, generalized statement about "the vital role that the public telephone has come to play in private communication" captures the Court's methodology for assessing the societal attitude towards Katz's expectation. Thus, post-Katz, the two-pronged reasonable expectation of privacy test seems to exist as an unbounded, ad hoc assessment by the Court of society's attitude toward the privacy interest at stake. In spite of *Katz*, it seems that many post-Katz courts have continued with some form of a property-based approach to determining the scope of the Fourth Amendment privacy.²⁹¹

²⁹⁰ *Supra* note. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

²⁹¹ See, for example, Kerr, "The Fourth Amendment and New Technologies," 823-827 (noting that very little has changed since Katz); Cloud, "Rube Goldberg Meets the Constitution," 20-36 concluding that

Kyllo v. United States

In 2001, the Supreme Court reaffirmed the core approach toward the Katz test when deciding *Kyllo v. United States*. In Florence, Oregon, the police had suspected that Kyllo was growing marijuana, a contraband substance at the time. To ascertain whether Kyllo was growing marijuana illegally in his home, the police used a thermal imaging device that was only available to them in order to measure heat emanating from high intensity lamps that Kyllo had placed to grow the plants.²⁹² Under these circumstances, the government and the device they utilized did not physically “enter” Kyllo’s house to determine if he was growing marijuana or measure heat released from his lamps.²⁹³ The government’s device measured the heat only after it had escaped from the house.²⁹⁴ Yet, the Court rejected a pure property-based analysis that was applied in making a decision about the Fourth Amendment’s right to privacy.

The Court found that the application of the heat measuring device intruded on the kind of privacy that the Fourth Amendment is meant to safeguard.²⁹⁵ The majority relied on specific words within the Amendment, such as whether “information” with the potential for acquiring intimate details exists; the “location,” meaning distance from the boundaries of a home; and use of the term “houses” was taken directly from the Fourth Amendment in order to make a determination on the extent of personal privacy. It

Katz is a failure if its original purpose was to regulate modern surveillance technologies with Fourth Amendment standards); Ku, “The Founders’ Privacy,” 1343-1362 (noting how post-Katz decisions have taken advantage of Katz’s failure to provide any real guidance on determining privacy values).

²⁹² *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

²⁹³ *Kyllo v. United States*, 533 U.S. 27, 29.

²⁹⁴ *Kyllo v. United States*, 533 U.S. 27, 30.

²⁹⁵ *Kyllo v. United States*, 533 U.S. 27, 40.

appears that their opinion is heavily influenced by the conventional perspective of property; it goes so far as to say that “in the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes.”²⁹⁶ Since the police did not trespass into Kyllo’s home, it can be expected that a pure property analysis would have yielded a different opinion from the Court. In their ruling, the *Kyllo* majority placed an emphasis on the police invasion of home-based intimacy, a personal privacy term, even though law enforcement officials had measured escaped heat outside Kyllo’s house.²⁹⁷ Had they ruled based on a purely property rights invasion point of view, the outcome could have been drastically different.

United States v. Jones

The U.S. Government obtained a search warrant permitting it to install a global-positioning-system (GPS) tracking device on a vehicle registered to Jones’s wife. The warrant authorized installation in the District of Columbia for up to ten days, but agents installed the device on the eleventh day and in Maryland. The U. S. Government then tracked the vehicle’s movements for twenty-eight days. It subsequently secured an indictment of Jones and others on drug trafficking conspiracy charges. The District Court suppressed the GPS data obtained while the vehicle was parked at Jones’s residence but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets. Jones was convicted. The D. C. Circuit

²⁹⁶ *Kyllo v. United States*, 533 U.S. 27, 37.

²⁹⁷ *Kyllo v. United States*, 533 U.S. 27, 38.

reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment.

The United States Supreme Court reaffirmed its commitment to evaluating the Fourth Amendment beyond the traditional scope of property analysis when it ruled in *United States v. Jones*.²⁹⁸ The whereabouts of Jones, a suspected drug trafficker, were monitored by the police for four weeks by surreptitiously installing a Global Positioning System (GPS) on the underside of his wife's car, which he was driving about.²⁹⁹ The police had not sought and obtained a search warrant on Jones, and all the Supreme Court justices recognized that it was an analysis that included the Katz test as a litmus, expressed in three sets of opinions. The majority, consisting of five members of the Court, found that Jones had a reasonable expectation to privacy when he was traveling in his car.³⁰⁰ This type of privacy would also be recognized by society as reasonable when the police were tracking Jones's public whereabouts over the course of four weeks in a privately-owned automobile registered in the name of Jones's wife.

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Here, the U.S. Government's physical intrusion on an "effect" for the purpose of obtaining information constitutes a "search." This type of encroachment on an area described in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. The Supreme Court's conclusion in *United States v. Jones* is

²⁹⁸ *United States v. Jones*, 132 S. Ct. 945, 951 (2012).

²⁹⁹ *Kyllo v. United States*, 533 U.S. 27, 948.

³⁰⁰ Justice Sotomayor found that such an expectation would exist if that issue had needed to be reached. *Kyllo v. United States*, 533 U.S. 27, 956. Justices Alito, Breyer, Ginsburg, and Kagan found that one did exist. *Ibid.*, 964.

consistent with its previous Fourth Amendment jurisprudence, which, until the latter half of the twentieth century, was tied to common-law trespass. Later cases, which have deviated from that exclusively property-based approach,³⁰¹ have applied the analysis of Justice Harlan's concurrence in *Katz v. United States*,³⁰² which said that the Fourth Amendment protects a person's "reasonable expectation of privacy."³⁰³ It appears that this shift in emphasis from property to privacy has come about gradually through a subtle interplay of substantive and procedural reform. The issue in this case was that the police had placed a GPS monitoring device on the underside of his car surreptitiously, after the warrant had expired. The Supreme Court of the United States ruled that this monitoring constituted a search that was protected by the Fourth Amendment.

Surreptitious DNA Harvesting and Privacy

The Katz test provides some insight into the framework of an analysis of the nature and scope of the Fourth Amendment's protection against the police practice of surreptitious DNA harvesting after it has left the body. One must consider whether the person whose DNA was harvested and analyzed had a reasonable expectation of privacy in their out-of-body DNA. Next, one must ask whether society's expectation would align with that of the individual and if they, too, are willing to recognize it as reasonable. Finally, we must collectively ask whether people expect their DNA to be secure from

³⁰¹ *Warden v. Hayden*, 387 U.S. 294, 304 (1967) where United States Supreme Court stated that "The premise that property interests control the right of the government to search and seize has been discredited. . . . We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts."

³⁰² *Katz v. United States* 389 U. S. 347.

³⁰³ *Katz v. United States* 389 U. S. 347, 360.

government and societal intrusion. If one views DNA through the lens of genetic privacy rather than as personal property, a powerful yet sophisticated shift occurs in our attitude and subsequent analysis of what is deemed reasonable expectation of privacy.

The abandonment question pivots on whether we were knowledgeable or intentionally sought to abandon that privacy. Under this metric, the abandonment of DNA is not consistent with an automatic disqualification of the Fourth Amendment. Now, its limited use of information contained within does not resolve the expectation question. As the privacy issue expands and takes into consideration a broader view of what privacy means to an individual and society in general, we can expect cases involving surreptitious harvesting of DNA to generate different outcomes.

Courts have also addressed the question of whether an individual has knowingly abandoned his or her right to genetic privacy. In the property or abandonment context, the Katz question now broadens from abandonment of bodily fluids, cigarette butts, or drinking cups to genetic privacy in DNA and one's expectation of privacy, according to the Fourth Amendment. One court wrote,

The distinction between abandonment in the property-law sense and abandonment in the constitutional sense is critical to a proper analysis of the issue. In the law of property, the question, as defendant correctly states, is whether the owner has voluntarily, intentionally, and unconditionally relinquished his interest in the property so that another, having acquired possession, may successfully assert his superior interest. In the law of search and seizure, however, the question is whether the defendant has, in discarding the property, relinquished his reasonable expectation of privacy so that its seizure and search is reasonable within the limits of the Fourth Amendment. In essence, what is abandoned is not necessarily the defendant's property, but his reasonable expectation of privacy therein.³⁰⁴

³⁰⁴ *City of St. Paul v. Vaughn*, 237 N.W.2d 365 (Minn. 1975).

This opinion suggests that abandonment requires knowledge and intention.³⁰⁵

Unless a person willfully and knowingly abandons his or her expectation of genetic privacy, no abandonment has taken place. Conversely, if people unknowingly abandon their expectation of genetic privacy, they are still entitled to privacy according to the Katz test and its application of the Fourth Amendment. The Katz Court appears to suggest the same notion, noting that “what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” Examples of Fourth Amendment protection involve circumstances when a defendant abandons contraband items³⁰⁶ or some other incriminating item³⁰⁷ upon seeing law enforcement officials approaching them or when fleeing the scene of the crime.³⁰⁸ In these situations, courts would debate whether the suspect’s acts, words, deeds, or objective facts showed a deliberate intention to abandon or not to; most of all the debate would be target towards examining whether there was any display of intention.³⁰⁹

In cases of *Bly*, *Cabral*, *Sigsbee* and others like them, there is ample evidence to show that suspects intentionally abandoned the straws, water bottles, and saliva.³¹⁰ However, there is no evidence to suggest that these suspects intended to abandon their

³⁰⁵ Mascolo, “The Role of Abandonment,” 401-402.

³⁰⁶ *State v. Britton*, 633 So. 2d 1208, 1209 (La. 1994) (hiding packet of cocaine in gun rack); *State v. Crandall*, 136 P.3d 30, 31 (Or. 2006) (hiding baggie underneath car).

³⁰⁷ *United States v. Collis*, 766 F. 2d 219, 220 (6th Cir. 1985) (abandoning airplane luggage after seeing DEA agents).

³⁰⁸ *United States v. Tugwell*, 125 F.3d 600, 602 (8th Cir. 1997) (walking away from suitcase at bus station after drug-sniffing dog alerts to it).

³⁰⁹ See, for example, *United States v. Jones*, 707 F.2d 1169, 1172 (10th Cir. 1983) (“[A]n expectation of privacy is a question of intent.

³¹⁰ See *supra* notes 58-62 and accompanying text.

genetic privacy when they left those items behind or placed them in a public trash receptacle.³¹¹ It would be speculative to conclude that those individuals were aware that, in abandoning those items, they had shed their DNA, which would subsequently be used for further sophisticated analysis and possibly glean other personal information, let alone used as a tool for identification. Through the use of newer appropriate technology by companies dedicated to DNA analysis, the scope and depth of genetic information that can be potentially obtained can be astounding. As biomedical research progresses, more personal information will be generated from DNA analysis.

Courts have ruled on other privacy in public cases, and they seem to support this type of analysis. In the *Katz* “garbage cases,” the likelihood that the owner is knowledgeable when discarding his or her garbage is considered. In *California v. Greenwood*, the Supreme Court found that “it is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public.”³¹² The alluded “common knowledge” that one’s shed DNA could include being accessible to the police, the use of sophisticated biotechnological tools for comparison to crime-scene samples or inclusion in a database, or both is information of which laypersons are typically not aware.

In other cases of privacy in public, courts have used a similar approach. Examples of fingerprint,³¹³ voice,³¹⁴ and handwriting³¹⁵ cases rest on individuals knowingly leaving

³¹¹ Note that the burden of proof in such circumstances is on the prosecution to justify their warrantless conduct. Mascolo, “The Role of Abandonment,” *supra* note 106, 403-404.

³¹² *California v. Greenwood*, 486 U.S. 35, 40 (footnotes omitted) (1988).

³¹³ See *Davis v. Mississippi*, 394 U.S. 721, 727 (1969) (“Fingerprinting involves none of the probing into an individual’s private life and thoughts that marks an interrogation or search.”).

them behind in public places to which others have open access. In *United States v. Jones*, the Supreme Court found that Jones had not abandoned his expectation of privacy by going out in public.³¹⁶ The fingerprint example is particularly significant because Elizabeth Joh has argued about the appropriateness of drawing parallels between surreptitiously harvesting out of body DNA versus secretly collecting fingerprints.³¹⁷ Superficially, the analogy appears attractive because, in each case, the police are expecting that the information they extract will reveal the identity of the perpetrator. However, that analogy need not necessarily hold true when “common knowledge” is also included in the equation. While it is common knowledge that touching an item with bare hands leaves fingerprints on it, the same cannot be asserted about out of body, shed DNA, even if its use is for identification, incorporation into a database, or both.

In *Kyllo*, the focus was police intrusion into home intimacy, which was measured as heat emanating from Kyllo’s home and the Supreme Court ruled that it was protected by the Fourth Amendment. Had the argument been posed differently, stating that the heat was considered abandoned or shed, the Court might not have found an issue with the police measuring the heat captured outside the protected area of the home. The Court might have ruled differently, and *Kyllo* may not have enjoyed the reasonable right to privacy, according to the Court's interpretation of the Fourth Amendment. Absent any

³¹⁴ See *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (“The physical characteristics of a person’s voice, its tone and manner . . . are constantly exposed to the public.”).

³¹⁵ See *United States v. Mara*, 410 U.S. 19,21 (1973) (“Handwriting . . . is repeatedly shown to the public.”).

³¹⁶ 132 S. Ct. 945, 950-951 (2012).

³¹⁷ Compare Joh, “Reclaiming ‘Abandoned’ DNA,” *supra* note 55, 871 (rejecting the appropriateness of the fingerprint analogy) with Kaye, “The Science of DNA Identification,” *supra* note 48, 420 (supporting the appropriateness of the fingerprint analogy).

evidence of *Kyllo*'s knowledge of the escaping heat and that it could reveal intimate details of activities inside his home with technology unavailable to the public, the Court majority might have ignored any possible abandonment analysis. Similarly, in a surreptitious harvesting case of "measurement" or analysis of out-of-body DNA by the police with technology unavailable to laypersons and without the knowledge or consent of the shedder, a Fourth Amendment violation could have occurred.

In surreptitious harvesting cases like *Sigsbee* and *Athan*, the question of proprietorship over out-of-body DNA was examined. These cases were also decided based on the *Katz* analysis and focused on whether intrusion of property and body took place. In these cases, Fourth Amendment protection was denied by the court because they determined that *Athan*'s bodily fluid, namely his saliva, was not taken using an intrusive procedure. In the Court's view, *Athan* voluntarily provided his DNA when he licked the envelope and mailed it back to the police. In this approach, departure from the body and its location rather than status of the DNA as property were taken into consideration.

Physical Boundaries

The question of physical boundaries of one's body can be explored further in the Fourth Amendment context when we examine *Schmerber v. California*. The police took a sample of *Schmerber*'s blood for blood alcohol analysis. Even though the invasion of *Schmerber*'s body was minimal and the equivalent to swabbing a mouth or scraping underneath nails, courts have held that invasion on a reasonable expectation to privacy occurred. The development of forensic DNA technology has begun to also cause questions as to what legally defines "body." Since cells invisible to the naked eye that are found outside the body can be confiscated for their DNA to be amplified and analyzed by

forensic scientists, the police can bypass intrusion into a body to gain access to genetic material. In this case, the out-of-body status would not eliminate any Fourth Amendment protection. However, the question remains whether out-of-body status of the DNA eliminates any Fourth Amendment protection.

Two cases possibly address the question of out-of-body Fourth Amendment protections for DNA. They are *Skinner v. Railway Labor Executives Association*³¹⁸ and *National Treasury Employees Union v. Von Raab*.³¹⁹

Skinner v. Railway Labor Executives Association

In 1985, after a number of railroad accidents in which alcohol or drugs were involved, the Federal Railroad Administration (FRA) adopted regulations that subjected employees involved in safety-sensitive work to blood and urine tests either for “reasonable cause” or after they were participants in a variety of specified major train accidents that involved deaths or damages of more than \$50,000 to railway property. Employees who refused to submit to testing were disqualified for “covered service” for nine months but were entitled to hearings about their refusals to cooperate.³²⁰

A number of labor organizations, including the Railway Labor Executives’ Association, filed suit. James Horace Burnley, the U.S. Secretary of Transportation, was initially a respondent. However, when Burnley left the post in 1989, Samuel K. Skinner, his successor, was named in the suit. A federal district court subsequently upheld the

³¹⁸ *Skinner v. Railway Labor Executives’ Association*, 489 U.S. 602 (1989).

³¹⁹ *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989).

³²⁰ *Skinner v. Railway Labor Executives’ Association*, 489 U.S. 602 (1989).

program's constitutionality, but the Ninth Circuit Court of Appeals reversed, finding that the program violated the Fourth Amendment which forbids unreasonable searches and seizure. The court objected to testing for drug and alcohol regardless of whether there was suspicion that employees engaged in their use.³²¹

The case was argued before the U.S. Supreme Court on November 2, 1988. On March 21 1989, *Skinner v. Railway Labor Executives' Association*, the U.S. Supreme Court ruled 7–2 that an alcohol and drug testing program for railroad employees in safety-sensitive positions did not violate the Fourth Amendment.³²² The court acknowledged that the disputed program constituted a “search” within the context of the Fourth Amendment insofar as the testing of railway employees was forced (not voluntarily provided) as a result of a governmental initiative. Therefore, the court was of the opinion that it was necessary to address the question of “reasonableness” in conducting the search. In other words, the court sought to review the balance between the intrusiveness of any drug test against the legitimate governmental interest of promoting safety. In doing so, the court relied on the concept of “special needs” outside normal law-enforcement channels in finding that the testing program was designed to be used in situations wherein the probable cause and warrant requirements simply were not feasible. The court further explained that though the Fourth Amendment's warrant requirement was designed to protect individuals' expectations of privacy, the regulations required testing only under clearly defined circumstances.³²³

³²¹ *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602 (1989).

³²² *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602 (1989).

³²³ *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602 (1989).

In *Skinner v. Railway Labor Executives Association*, institutional regulations mandated testing of employees for drug and alcohol through urine analysis. The collection of a urine sample would involve in-person monitoring, but no physical intrusion was permitted. Despite the lack of bodily intrusion, the U.S. Supreme Court found that the collection and testing of urine intrudes upon an individual's reasonable expectation of privacy that society has long recognized as such. The Court directly addressed the lack of bodily intrusion as:

It is not disputed, however, that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic. Nor can it be disputed that the process of collecting the sample to be tested, which may in some cases involve visual or aural monitoring of the act of urination, itself implicates privacy interests.³²⁴

For the *Skinner* Court, government's lack of bodily intrusions did not inevitably eliminate the possibility of a reasonable expectation of privacy in the out of body fluids and their content, unlike what was ruled in surreptitious harvesting cases.³²⁵ There are few activities in our society more personal or private than the passing of urine. Most people describe it by euphemisms, if at all they decide to discuss this topic. It is a function that is typically very private and performed without any public observation. In fact, in most societies, its performance in public is prohibited by law and social custom.³²⁶

³²⁴ *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602, 606 (1989).

³²⁵ *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602, 617. See also generally Alfano, "Note, Look What Katz Leaves Out" (arguing for an expansive view beyond bodily intrusion for what constitutes a search).

³²⁶ 816 F.2d 170, 175 (5th Cir. 1987), *aff'd in part, rev'd in part*, 489 U.S. 656 (1989).

National Treasury Employees Union v. Von Raab

The United States Customs Service (currently the U.S. Customs and Border Protection) is a federal agency charged with protecting the borders of the United States.³²⁷ In May 1986, defendant William von Raab, who was also the commissioner of the Service, implemented a new drug-testing program. This program made successful drug testing a pre-requisite for employees seeking to be promoted to three categories of positions:

1. positions directly involved with the interdiction of illegal drugs,
2. positions requiring the carrying of firearms in the line of duty, and
3. positions with access to classified material.

Under the program, an employee who tested positive without a legitimate explanation was subject to dismissal. The plaintiff in this case, The National Treasury Employees Union, challenged the drug-testing program on the basis that the mandated program violated the privacy of employees and, therefore, infringed upon any reasonable expectation of privacy as per the Fourth Amendment.³²⁸ The district court enjoined the program, and the U.S. Court of Appeals vacated the injunction. The United States Supreme Court granted *certiorari*.³²⁹

The possibility that a person might have a reasonable expectation of privacy of the sort that society is willing to recognize in out-of-body DNA does not resolve the issue. It is possible that the sense of genetic privacy that an individual recognizes in one's

³²⁷ See the U.S. Customs and Border Protection web site at <https://www.cbp.gov/about>.

³²⁸ See, for example, <https://law.jrank.org/pages/23465/National-Treasury-Employees-Union-v-Von-Raab-Significance.html>

³²⁹ *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989).

out-of-body DNA is not consistent with the expectation of privacy that society is willing to recognize, as it did in the privacy “flowing” from urine in *Skinner* and as also defined, albeit partly, in another mandatory urinalysis case, *National Treasury Employees Union v. Von Raab*. The United States Supreme Court has observed,

There are few activities in our society more personal or private than the passing of urine. Most people describe it by euphemisms if they talk about it at all. It is a function traditionally performed without public observation; indeed, its performance in public is generally prohibited by law as well as social custom.³³⁰

Out of Body DNA Collection

Courts have ruled against the right to privacy over one’s DNA and argued that the out-of-body DNA obtained by the police was purely for limited use of the information extracted from the genetic material. The right to reasonable expectation of privacy regarding personal information was addressed in one of the surreptitious harvesting cases. The *Athan* court ruled that the defendant’s Fourth Amendment privacy was not violated because the use of his out of body DNA was “narrowly limited to identification purposes.”³³¹

Professor David Kaye asserts that the use of out-of-body DNA is no different than that if one were utilizing fingerprints for identification purposes. This assertion is based on the premise that analysis of STR DNA testing has no more personal information than

³³⁰ Solove and Schwartz, “Information Privacy Law,” 1040. 816 F.2d 170, 175 (5th Cir. 1987), *aff’d in part, rev’d in part*, 489 U.S. 656 (1989).

³³¹ *State v. Athan*, 158 P.3d 27, 34 (Wash. 2007). The court’s conclusion was contrary to an assertion by the ACLU that out-of-body DNA “has the potential to reveal a vast amount of personal information, including medical conditions and familial relations.” *Ibid*.

a fingerprint. This is a view that is also shared by other scholars.³³² However, this analysis has the same disadvantage and narrow scope that has plagued courts' intrusion on property and intrusion on body analysis. If the analytical focus is purely on expectation of privacy rather than on the information encoded in the DNA, one also considers the potential information that could be obtained by the police and an individual's concern for its potential use. This argument is challenged by the *Athan* court and David Kaye where they assert that intrusion on the expectation of privacy is impossible in out-of-body DNA harvesting by the police and its subsequent analysis because the information obtained is limited as it is in fingerprinting and, therefore, can only have restricted use.³³³

That DNA obtained by law enforcement has limited use is inconsistent with the rulings in *Kyllo* and *Skinner*. In *Kyllo*, the suspect was thought to be growing marijuana illegally in his house with the aid of energy lamps from which heat was detected escaping his home through the use of thermal imaging technology available only to the police at that time.³³⁴ Although this finding implicated *Kyllo* in an unlawful act, the Court ruled that he had a reasonable expectation of privacy because the thermal detection device used by the government in generating evidence against *Kyllo* was intrusive and capable of detecting intimate details inside his home.³³⁵ The court was explicit and rejected "limiting

³³² Kaye, "Science Fiction and Shed DNA," 409, 420; Cole, "Is the 'Junk' DNA Designation Bunk?," at <http://www.northwesternlawreview.org/online/%E2%80%9Cjunk%E2%80%9D-dna-designation-bunk>; see generally Kaye, "Please, Let's Bury the Junk" (in response to Cole).

³³³ Imwinkelried and Kaye, "DNA Typing: Emerging," 436-440; Kaye, "Science Fiction and Shed DNA," 64-65. See also Kaye, "Please, Let's Bury the Junk," 71.

³³⁴ *Kyllo v. United States*, 533 U.S. 27, 29-30 (2001).

³³⁵ The Court rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth.

the prohibition of thermal imaging to ‘intimate details.’” In *Skinner*, the court ruled on an employer-mandated chemical test of urine to detect drugs and alcohol in employees and said, “chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic. Nor can it be disputed that the process of collecting the sample to be tested, which may in some cases involve visual or aural monitoring of the act of urination, itself implicates privacy interests.”³³⁶ The potential for obtaining personal information over and above the original intention created an expectation of privacy in both *Skinner* and *Kyllo*.

Science and Technology

The traditional thirteen CODIS core loci DNA testing generates sufficient genetic information to essentially identify an individual, enabling police to rule out or identify a suspect in a crime. More recently, even more autosomal STR loci can be typed using commercially available testing kits, along with Y-chromosome STR kits and mtDNA sequencing methods. These procedures could potentially intrude on other individuals’ expectations of privacy as an unintended consequence of the DNA identification process. The provisions of the U.S. Combined DNA Index System (CODIS), a series of local, state, and national databases, legally permits the Federal Bureau of Investigations (FBI) and state and local law enforcement agencies to include records of DNA identifications

Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development. *Kyllo v. United States*, 533 U.S. 27, 35–36.

³³⁶ 489 U.S. 602, 606 (1989), 617.

of persons who voluntarily submit their DNA samples collected “under applicable legal authorities” for the purpose of excluding them from a crime (i.e., exclusion samples).

Even if one only relies on a genetic fingerprint generated by the standard 13-loci DNA test, the potential for intrusions on an individual’s expectation of privacy could presumably exist beyond that associated with a traditional fingerprint. For example, the provisions of the Federal CODIS database legislation permit the inclusion of DNA identification records of “other persons whose DNA samples are collected under applicable legal authorities, provided that DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System.”³³⁷ This statement suggests that one’s harvested genetic nametag will appear in the Federal CODIS database as long as such harvesting is conducted according to First Amendment guidelines.

Once in the database, the individual’s DNA, whether guilty or innocent of a crime, may become subject to a coincidental match with a crime scene sample or a partial match and where such a match that would likely require an explanation. In case of a partial match, it may lead to a court authorized search of the family members’ genetic profiles.³³⁸ That individual may also be the subject of an erroneous match, intentional or otherwise. The aforementioned edict indicates that a person’s harvested DNA nametag can make its way into CODIS provided the DNA collection is constitutional. Under these

³³⁷ 42 U.S.C. § 14132(a)(1)(C) (2006).

³³⁸ Bieber et al., “Finding Criminals through DNA,” 1315; Paoletti et al., “Assessing the Implications,” 161; Nakashima, “From DNA of Family,” A01.

circumstances, this DNA could become a target of various mishaps in an identification process, such as a false match or partial match, whether it is erroneous or otherwise.³³⁹

DNA collected under unregulated conditions where its storage is not undertaken using carefully controlled guidelines has the risk of becoming misused or mismanaged. Similarly, one can envision the increased opportunity for mishandling genetic information when it is gathered surreptitiously or by amateur genealogists. Hypothetically, the DNA could get included among “rogue” or “linkage” databases of suspects or along with other unregulated databases or profiles.³⁴⁰ In this scenario, DNA can be analyzed beyond its homology in the thirteen loci examined in STR testing to yield much more information than the owner had been led to believe. DNA can be analyzed for congenital diseases, diseases acquired by genetic mutations, ethnic origin, skin color, gender, and behavioral pre-dispositions, including sexual orientation.³⁴¹

Although there is no evidence that such conduct is taking place directly from government laboratories, the purchase of genetic data by private, for-profit institutions may not be completely farfetched. With the use of samples that have been obtained from a search that is protected by the Fourth Amendment, clandestinely or volunteered, the possibility of “function creep” could exist.³⁴² That society would recognize these hypothetical possibilities of DNA misuse and recognize them as intrusions on expectation of privacy remains to be seen due to the complex nature of this topic.

³³⁹ Saks and Koehler, “The Coming Paradigm Shift,” 892.

³⁴⁰ Willing, “Authorities Find More Uses,” at <http://usatoday30.usatoday.com/>.

³⁴¹ See *United States v. Kincaid*, 379 F.3d 813, 849–51 (9th Cir. 2004) (Reinhardt, J., dissenting) addressing potential scope of DNA identification given advancing technology); Matejik, “DNA Sampling: Privacy and Police,” 53, 59.

³⁴² Simoncelli and Steinhardt, “California’s Proposition 69,” 199, 201–04.

The out-of-body status of surreptitiously harvested DNA does not automatically resolve the question of reasonable expectation of privacy. When the focus is upon intrusion on privacy, the scope for interpretation is broadened. The abandonment question now becomes whether an expectation of privacy is also relinquished rather than just an object. The very limited STR identification information and its equally limited current use broaden into a wider selection of possible genetic information and its use. A thorough reasonable expectation of privacy analysis must, therefore, consider the nature and scope of DNA or genetic privacy. However, that expansion in thinking does not automatically provide an easy answer.³⁴³ Further along, I will discuss crafting a preliminary outline of an expectation of genetic privacy that society might be also willing to recognize as reasonable and consider providing their support.

Understanding Privacy

Privacy can be a multi-dimensional, nebulous concept and viewed differently by members in a society, depending on socioeconomic disparities. To weave the notion of genetic privacy into the Fourth Amendment, an understanding of privacy is necessary. On December 15, 1890, Samuel Warren and Louis Brandies published a seminal article, titled “The Right to Privacy” in the *Harvard Law Review* in which they formulated the

³⁴³ An explanation of why courts have so consistently misapplied *Katz* in surreptitious harvesting cases is slightly off topic, although related. At least three plausible explanations exist for this overly narrow approach: (1) It seems like a fingerprint; some people call it “DNA fingerprinting”; let’s treat it like a fingerprint; (2) All surreptitious harvesting cases to date have involved what I have referred to as putative suspects, (i.e., someone for whom the police have some suspicion but not enough to get a search warrant). It is plausible that at least at subconscious level, a judge has thought, “it’s not as if we’re talking about the privacy of a ‘completely’ innocent person” and has allowed the bias to restrain the depth of the analysis; and (3) The average laypersons, including judges, likely have little knowledge and even less understanding of the possible meaning of genetic information we are acquiring at a rapid rate. To expect judges to base their judgment on an assessment of the nature and scope of genetic privacy is also asking them to accomplish a very difficult task.

concept of the right to privacy principally as the right to be left alone. Projecting far into the future, Warren and Brandeis lament the “[i]nstantaneous photographs and newspaper enterprise [that] have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”³⁴⁴ Since then, other definitions have been added to a growing list of privacies, depending on arising and increasing societal needs.

Privacy has now been also defined as limited access to the self and the ability to shield oneself from unwelcome access by others. There is also a component of secrecy associated with privacy, along with the desire to conceal, protect and shield information. Privacy could also mean unwillingness to share information about oneself. In contemporary times, the meaning of privacy could expand into protection of one’s personality, individuality, lifestyle preferences, and dignity. Privacy also suggests intimacy, where there is control over or limited access to one’s intimate relationships or personal aspects of life.

The Road to Genetic Privacy

The U.S. Supreme Court has defined the concept of a constitutional right to privacy from numerous perspectives reaching beyond the formal boundaries of the original Fourth Amendment text. Several landmark cases have led to the evolution of a societal understanding and expectation of privacy from what we do with our bodies to whom we decide to legally wed. In *Griswold v. Connecticut*, the Supreme Court

³⁴⁴ Warren and Brandeis, “The Right to Privacy,” 193.

addressed a woman's right to privacy and birth control, ruling that a state's ban on the use of contraceptives violated the right to marital privacy. The case concerned an 1879 Connecticut law that criminalized the encouragement or use of birth control. *Roe v. Wade* was another landmark legal case in which the U.S. Supreme Court on January 22, 1973, ruled (7–2) that unduly restrictive state regulation of abortion is unconstitutional. In a majority opinion written by Justice Harry A. Blackmun, the court held that a set of Texas statutes criminalizing abortion in most instances violated a woman's constitutional right to privacy.

In 1977, *Whalen v. Roe* was a case brought before the Supreme Court of the United States in which the constitutional right to informational privacy was granted, and the Court ruled that patients have the right to privacy over their prescription medication information as a matter of due process.³⁴⁵ This was possible because the Court reversed the District Court, holding that the New York State Statutes requiring the collection and storage of a patient's identifying information did not violate a citizen's constitutional right to privacy, and it is within the State's police power to collect such information in an attempt to stop illegal drug distribution. *Whalen v. Roe* suggests a constitutional right to informational privacy as a matter of due process.³⁴⁶

³⁴⁵ *Griswold v. Connecticut*, 381 U.S. 479, 485–86 (1965) (holding state law forbidding use of contraceptives unconstitutional because it intruded upon right of marital privacy); *Roe v. Wade*, 410 U.S. 113, 153 (1973) (holding right to privacy broad enough to encompass woman's decision whether to terminate pregnancy under Ninth or Fourteenth Amendment); *Lawrence v. Texas*, 539 U.S. 558, 564 (2003) (holding state law criminalizing some consensual same-sex sex acts unconstitutional under the Due Process Clause of Fourteenth Amendment); *Whalen v. Roe*, 429 U.S. 589, 605–06 (1977) (recognizing Fourteenth Amendment concerns over disclosure to state of prescriptions to certain drugs but ultimately holding no violation of such rights or liberties).

³⁴⁶ *Whalen v. Roe*, 429 U.S. 589, 605–06, *supra* note 65 (1977) (recognizing Fourteenth Amendment concerns over disclosure to state of prescriptions to certain drugs but ultimately holding no violation of such rights or liberties).

The cases emanating from the Fifth Amendment's prohibition on self-incrimination effectively describe a privacy right grounded in one's personal dignity.³⁴⁷ More recently, in *Lawrence v. Texas* (2003), the United States Supreme Court ruled that state laws banning homosexual sodomy are unconstitutional as a violation of the right to privacy. The Court overturned a Texas anti-sodomy law as a violation of the right to privacy and the Equal Protection Clause of the Fourteenth Amendment. Thus, the ruling in *Lawrence v. Texas* expands the original view of privacy and protects certain personal decisions and behavior from governmental intrusion implicit in a number of constitutional amendments.

In 2005, in a *California Law Review* article titled "Conceptualizing Privacy," Daniel J. Solove of George Washington School of Law placed contemporary expectations of privacy in six distinct categories. They are

1. the right to be left alone: Samuel Warren and Louis Brandeis's famous formulation for the right to privacy;
2. limited access to the self: the ability to shield oneself from unwanted access by others;
3. secrecy: the concealment of certain matters from others;
4. control over personal information: the ability to exercise control over information about oneself;
5. personhood: the protection of one's personality, individuality, and dignity; and

³⁴⁷ *Miranda v. Arizona*, 384 U. S. 436, 457 (1966) (finding the interrogation environment to be "destructive of human dignity"); *Schmerber v. California*, 384 U. S. 757, 762 (1966) ("[T]he constitutional foundation underlying the privilege is the respect a government—state or federal—must accord to the dignity and integrity of its citizens.").

6. intimacy: control over, or limited access to, one's intimate relationships or aspects of life.³⁴⁸

Conceptually, genetic privacy could fit into each one of Solove's six categories.³⁴⁹ However, there is no record showing that the U.S. Supreme Court has directly addressed genetic privacy in cases involving intrusions on a right to genetic information, whether it is in the informational, decisional, behavioral, or dignitary categories.³⁵⁰ With broader conceptions of privacy, one can envisage how genetic privacy straddles some of the variants of constitutional privacy in the all categories.

As the Human Genome Project was conceived and began to take shape, genetic privacy increasingly became a topic of interest among scholars in several disciplines, each of whom has defined conceptions of genetic privacy from their individual perspective.³⁵¹ Bioethicists and moral philosophers have examined genetic privacy in moral terms.³⁵² Many others have proposed model genetic privacy legislation,³⁵³ and

³⁴⁸ Solove, *Understanding Privacy*, 12–13. Solove argues persuasively that none of these conceptions captures the common denominator of privacy; *Ibid.*, 14, and goes on to propose a “taxonomy of privacy” that seeks to provide a better understanding of privacy; *Ibid.*, 101–02.

³⁴⁹ Solove, *Understanding Privacy*, *supra* note.

³⁵⁰ Though, as a scientific matter, gender-discrimination cases are arguably genetic privacy cases.

³⁵¹ See generally Allen, “Genetic Privacy: Emerging Concepts,” 31 (discussing various definitions of “genetic privacy” and the legal and ethical values of each).

³⁵² See, for example, Zimmerli, “Who Has the Right,” 93 (discussing genetic privacy from “information ethics” point of view and suggesting perhaps under such view there is no right to private ownership of any kind of information).

³⁵³ See generally Annas et al., *The Genetic Privacy Act* (proposing federal legislation to address the privacy concerns relating to genetic information in light of the Human Genome Project).

legislators have passed numerous versions of such legislation.³⁵⁴ Research scientists and health care professionals have grappled with practical applications of conceptions of genetic privacy, and several legal scholars have also addressed the issue.³⁵⁵ Considering the interest among various scholars, it is possible that a right to genetic privacy could become an Amendment in the Constitution and included as a human right.

When the Genetic Information Nondiscrimination Act (GINA) was signed into law by President George W. Bush in 2008, it was considered was unusually forward-looking; it protected against a form of discrimination that was not yet common. Under this Federal law, employers and health insurance companies could not request the genetic test results of an individual or that individual's family members and discriminate based upon them. Nor can this information be used for decisions regarding coverage, rates, or preexisting conditions. Employers cannot use genetic information for hiring, firing, or promotion decisions, or any other decisions regarding employment.³⁵⁶ To clarify, genetic information includes the following:

1. an individual's genetic tests (including those done as a part of research studies),
2. genetic tests of the individual's family members (dependents and up to and including 4th degree relatives),

³⁵⁴See the National Conference of State Legislators' website for a comprehensive catalog of state-by-state genetic-privacy legislation, at <http://www.ncsl.org/issues-research/health/genetic-privacy-laws.aspx>.

³⁵⁵ Several journals have dedicated symposium-style issues to the topic. For example, *Texas Review of Law & Politics*, "Symposium, Technological Innovation & Legal Tradition" (discussing various viewpoints on the treatment of genetic information); *Jurimetrics Journal*, "Symposium, Respecting Genetic Privacy" (proposing a coherent theme for genetic privacy). See generally Wertz et al., *Guidelines on Ethical Issues* (discussing genetic-privacy issues in light of the Human Genome Initiative from the perspective of healthcare professionals).

³⁵⁶ See Genetics Generation, "Genetic Information Nondiscrimination Act of 2008," at <http://knowgenetics.org/genetic-information-nondiscrimination-act-of-2008-gina/>

3. genetic tests of any fetus or embryo of the individual or of a family member,
4. a disease or disorder affecting family members (family history) and
5. the results of genetic services and participation that includes genetic services for the individual or for a family member.

However, it is important to note that GINA does not apply to the following:

1. employers with 15 or fewer employees
2. members of the military or veterans' healthcare
3. extend to life insurance, disability insurance, and long-term care insurance
4. extend to diseases or disorders that individuals have been diagnosed with
5. mandate coverage for any particular test or treatment

In addition, other tests like blood counts, cholesterol tests, and liver-function tests, are not protected under GINA. If an employer does have an employee's genetic information, the employer must keep it confidential and in a separate file. It should be mentioned that the employment provisions of GINA³⁵⁷ prohibit employers from requiring or requesting an individual to undergo genetic testing or disclosing the results of a genetic test as a pre-requisite to employment.³⁵⁸ Nevertheless, GINA does not affect a key provision of the Americans with Disabilities Act (ADA),³⁵⁹ under which an employer may, after a conditional offer of employment, lawfully require an individual to sign an

³⁵⁷ *GINA* § 102(b).

³⁵⁸ *GINA* § 202.

³⁵⁹ 42 U.S.C. §§ 12101–12213.

authorization to disclose all of his or her health records to the employer.³⁶⁰ Individuals with a genetic predisposition to future illness are probably not covered by the ADA. Nothing in the ADA Amendments Act indicates any congressional intent to overrule existing Supreme Court precedent holding that before an asymptomatic condition can be covered under the ADA, it must limit a major life activity.³⁶¹

Companies that sell genetic tests and related products or services expressed their support of GINA, noting that consumers no longer need to worry about genetic testing. According to Amy DuRoss, head of Policy and Business Affairs at Navigenics, a genomics company based in Redwood Shores, California, “Having federal protection sends a message that the future is now for technology related to genetic information.” Similarly, Patrice Milos, CSO of Boston-based Helicos BioSciences, said, “I am confident the public will take this as a positive signal...this shows we have an informed Congress now. They are knowledgeable about what the future of genomics holds.”³⁶²

The hope is that by increasing consumer protection and safeguarding their genetic privacy, GINA will alleviate their doubts and fears towards genetic testing. California based genetic testing companies like 23andMe and Navigenics began launching DNA testing services that would help consumers check their genome to assess and address any risks for disease.³⁶³ Navigenics’s \$1,000 service offers only health-related information and not genealogical data unlike 23andMe. Navigenics also offers genetic counseling to

³⁶⁰ 42 U.S.C. § 12112 (d)(3).

³⁶¹ See *Bragdon v. Abbott*, 524 U.S. 624 (1998) (asymptomatic, HIV-positive patient denied dental services in dentist’s office was covered under Title III of the ADA because, for her, being HIV-positive was a substantial limitation on the major life activity of reproduction).

³⁶² Allison, “Is Personalized Medicine Finally Arriving?” 509-517.

³⁶³ <https://www.23andme.com/>.

help people understand their test results.³⁶⁴ As of 2012, Navigenics was purchased by Life Technologies and is subsequently no longer in existence in its original independent capacity.³⁶⁵ Similarly, Myriad Genetics, which tests for mutations implicated in BRCA1, BRCA2 genes as well as genetic mutations leading to ovarian cancer, hailed the potential of GINA towards benefiting those at risk. Oren Cohen, Senior Vice President of Clinical Research Strategies at CRO Quintiles Transnational stated, “The BRCA test is one I’d expect to become much more sought-after now.”³⁶⁶ Others, too, like David Resnick, a partner at the Boston-based law firm Nixon Peabody, echo these sentiments, quoting a personal story of at-risk family members who stood to benefit from GINA’s promise of anti-discrimination and discretion. “There’s pent-up demand for that test, because there was widespread fear of discrimination,” said Resnick.³⁶⁷

In spite of the eagerness expressed by profit seeking companies, members of academia expressed caution toward accepting GINA as a genetic privacy panacea and distrust towards profit motivated companies that have embraced it quickly. Although GINA is a monumental accomplishment, according to Rudi Tanzi, Professor of Neurology at Harvard Medical School and Director of the Genetics and Aging Unit at Massachusetts General Hospital in Boston, Massachusetts, “we need to remember that this is just one step.”³⁶⁸ Ostensibly, critics of the bill share a different point of view. They

³⁶⁴ Pollack, “Is a DNA Scan,” at <https://www.nytimes.com/2010/03/20/business/20consumergenebar.html>.

³⁶⁵ GenomeWeb, “Life Technologies Acquires Consumer,” at <https://www.genomeweb.com/diagnostics/life-technologies-acquires-consumer-genetics-testing-firm-navigenics#.XQZacrXkHPY>.

³⁶⁶ Allison, “Trouble at the Office”; *Supra* note 245, 597.

³⁶⁷ Allison, “Industry Welcomes Genetic Information,” 596-597.

³⁶⁸ *Supra* note 245; Allison, “Trouble at the Office,” 597.

are of the opinion that that GINA is both unnecessary and burdensome to employers who must now be extra cautious in inadvertently divulging any genetic information, according Allison.³⁶⁹ However, misgivings about GINA would do little to assuage the fear of employment discrimination, retribution, or health insurance loss as a reason to avoid genetic testing, even if a doctor recommends such tests.

Amy DuRoss, formerly of Navigenics supports the passage of GINA. She comments, “Some people say there hasn’t been any discrimination, so why bother having a law? But the perception of risk is just as real a problem as actual discrimination. People did not feel safe.”³⁷⁰ By placing safeguards to protect the confidentiality of personal genetic information would boost confidence among potential consumers and patients. Therefore, GINA’s passage should, in theory, propel demand for consumer-directed tests and personalized medicine and a willingness to enroll in clinical trials that require genetic information, further down the road. Raju Kucherlapati, a Professor at Harvard Medical School and Director of the Boston-based Harvard-Partners Center for Genetics and Genomics, noted, “If people hear a trial uses an electronic medical record, they are afraid the information will get to their insurance company and they could be discriminated against.”

The degree of privacy through the passage of GINA could potentially send a ripple effect across many fields because “there is increasing recognition that genetics plays an important role in all aspects of human health and disease,” according to Kucherlapati. However, some experts caution that consumers are receiving information

³⁶⁹ *Supra* note 245; Allison, “Trouble at the Office,” 597.

³⁷⁰ Allison, “Trouble at the Office”; *supra* note 245, 597.

about risks that are still being ironed out. It seems that companies dedicated to genetic analyses are more interested in capitalizing on the probable increase in privacy that GINA offers as quickly as possible. “These companies are popping up like spring flowers to make money on genetics,” Tanzi says. “They should be helping to fill in all the blanks instead.”³⁷¹

This thesis discusses the nature and scope of genetic privacy and its relationship with the Fourth Amendment given the possibility that out of body DNA may be harvested and become public property. This paper also examines whether genetic privacy is a concept that society is willing to recognize and want to protect as a fundamental right. Direct Fourth Amendment jurisprudence as to whether one has an expectation of genetic privacy is limited. Courts frequently consider cases in which arguments are made based on different versions of bodily integrity, physical, property, and informational privacy when faced with a genetic privacy circumstance. A few courts also hint at an additional kind of less tangible privacy at stake in genetic privacy cases, one that will be discussed later as a dignitary-privacy concern.³⁷² However, it seems that none develop the full portrait of multi-dimensional genetic privacy.

³⁷¹ *Supra* note 169; Allison, “Industry Welcomes Genetic Information,” 596-597; *supra* note 245; Allison, “Trouble at the Office.”

³⁷² See *infra* Part V.B.3.

Chapter III.

Reasonableness of Expectations of Genetic Privacy

To date, there are two opinions on surreptitious harvesting that come close to addressing society's notion of the reasonableness of an expectation of genetic privacy. First, the *Christian* court found that the defendant did not have an objective expectation of privacy in the DNA "in the absence of any definitive authority to the contrary."³⁷³ Second, the *Sigsbee* court dismissed the idea of any expectation of privacy in bodily fluids as opposed to an item on which the fluids was found. They stated, "such theory would prohibit any and all testing upon items obtained from an individual regardless of whether they were lawfully or unlawfully obtained. This is not only an unacceptable premise, but also would be an unreasonable extension of an individual's expectation of privacy absent any legitimate constitutional basis."³⁷⁴ Both the *Christian* and *Sigsbee* courts chose not to characterize the nature or scope of society's conception of reasonable genetic privacy before dismissing the idea.

³⁷³ *State v. Christian*, No. 04-0900, 2006 WL 2419031, at *4 (Iowa Ct. App. Aug. 23, 2006). The *Athan* court found "no inherent privacy interest in saliva" and chose not to address any possible significant privacy interest in DNA because "the State's use of Athan's DNA here was narrowly limited to identification purposes." *State v. Athan*, 158 P.3d 27, 33-34 (Wash. 2007).

³⁷⁴ *People v. Sigsbee*, No. 03-0342, slip op. at 33 (Onondaga, N.Y. Cnty. Ct. Oct. 30, 2003). The *Sigsbee* court failed to appreciate that, even if one recognized an expectation of privacy in one's DNA that society was willing to recognize as reasonable, it would mean only that the police would be required to justify their search by showing probable cause or some other quantum of evidence. It would not "prohibit any and all testing."

Genetic Database Opinions

Courts have also addressed a broad conception of Fourth Amendment genetic privacy in the extensive litigation related to the constitutionality of investigative genetic databases. Because those cases invariably involve mandatory collection of samples and body intrusions, such as buccal swabs or drawn blood samples, most courts do no formal Katz search analysis.³⁷⁵ Nonetheless, in their analysis of the reasonableness of the search, several genetic-database courts have taken the opportunity to describe the nature of the privacy interest at stake when the government acquires an individual's DNA. Some courts have used a totality-of-the-circumstances balancing test, where there was probable cause of a criminal act in order to assess the reasonableness of the search that involved in obtaining a sample of blood or saliva.³⁷⁶ That test asks the court to balance the nature of the privacy interest at stake and the degree of intrusion on that interest against the importance of the governmental interest at stake.³⁷⁷

Genetic-database opinions that have directly evaluated the nature of the privacy interest at stake have often based that interest in well-established privacy conceptions that include bodily integrity, informational integrity, or both. Most commonly, in genetic-database opinions that were focused on bodily integrity, and where the degree of physical intrusion into the body was in question, courts have compared it to that of taking blood,

³⁷⁵ See, for example, CONN. GEN. STAT. ANN. § 54-102g(a)–(e) (West 2009) (compelling certain offenders to give DNA samples).

³⁷⁶ For example, *United States v. Sczubelek*, 402 F.3d 175, 182–84 (3d Cir. 2005) (analyzing all relevant facts to determine whether it is reasonable to demand that convict give DNA sample).

³⁷⁷ *United States v. Sczubelek*, 402 F.3d 175, 182. See *Landry v. Attorney Gen.*, 709 N.E.2d 1085, 1090–92 (Mass. 1999) (holding involuntary collection of DNA from persons convicted of certain crimes was not unreasonable search and seizure because it involved little risk or pain and government's interest in making record of convicts was strong).

fingerprints, or photographic samples.³⁷⁸ Some of those courts used those physical-intrusion analogies as the only basis for their conceptualization of genetic privacy, whereas others used them as a supplement to information-intrusion analogies. Both types of courts ruled that an individual's genetic privacy had no greater scope than the kind of narrow physical privacy at issue as with drawing blood or lifting fingerprints.³⁷⁹

Courts that focused primarily on the informational conception of genetic privacy also relied on analogies to other well-established areas of privacy. Some referred to the intrusion on information as akin to obtaining a fingerprint,³⁸⁰ whereas others discussed intrusion more broadly as identity information where the state was solely interested in establishing an individual's identity or determining the individual's identity by comparing it to two or more fingerprints.³⁸¹ In either case, courts' opinions of genetic privacy were singularly based on previously asserted limited use reason. They stated that they viewed genetic privacy and the information obtained after analysis as solely utilized for identification purposes, just like routine fingerprinting of a suspect. The concept of

³⁷⁸ For example, *Padgett v. Ferrero*, 294 F. Supp. 2d 1338, 1342 (N.D. Ga. 2003) (“The bodily intrusion of taking a blood or saliva sample is minimal. It is not significantly greater than taking fingerprints or a photograph.”).

³⁷⁹ *Padgett v. Ferrero*, 294 F. Supp. 2d 1338, 1342 (N.D. Ga. 2003).

³⁸⁰ See *Green v. Berge*, 354 F.3d 675, 680 (7th Cir. 2004) (“Use of DNA is in this respect no different from use of a fingerprint; only the method of obtaining the information differs, and for prisoners that is a distinction without importance.”); *Boling v. Romer*, 101 F.3d 1336, 1340 (10th Cir. 1996) (approving “use of DNA in a manner not significantly different from the use of fingerprints”); *Vanderlinden v. Kansas*, 874 F. Supp. 1210, 1215 (D. Kan. 1995) (“[T]he court finds persuasive the . . . analogy of the blood and saliva gathering at issue here to traditional identification techniques, such as fingerprinting.”); *People v. Wealer*, 636 N.E.2d 1129, 1137 (Ill. App. Ct. 1994) (“[W]e consider the sampling mandated . . . as functionally equivalent to fingerprinting . . .”).

³⁸¹ See, for example, *Groceman v. U.S. Department of Justice*, 354 F.3d 411, 413 (5th Cir. 2004) (“[L]ike fingerprinting, collection of a DNA sample for purposes of identification implicates the Fourth Amendment”); *Miller v. U.S. Parole Commission*, 259 F. Supp. 2d 1166, 1178 (D. Kan. 2003) (“The DNA sample is used solely to provide identification information and that purpose, and no other, is articulated in 42 U.S.C. § 14135e. DNA identification is often likened to a fingerprint. While some differences exist, they are both identity markers.”)

genetic privacy as information-based had no greater scope or depth other than that, according to these courts.

It is not surprising that these courts would view genetic privacy either in the physical privacy or limited-information privacy sphere. The impetus of courts in considering the full dimension of all that genetic privacy encompasses was abstract at this point in time. Their views were formulated in the context of weighing components that are challenging to quantify, such as governmental interest, the nature of privacy interest, and the degree of personal intrusion that they bring about.³⁸² The courts were assessing statutory structures that superficially had the appearance of earlier physical characteristics like collection of information for identification purposes only, just like photographs and fingerprints have been routinely used in criminal cases.³⁸³

It is surprising that there are genetic-database opinions that show signs of breaking away from the classic, narrow physical intrusion and information-intrusion paradigms to cast a wider dimension on the concept of genetic privacy. In some instances, these courts merely considered and then rejected a broader concept of genetic privacy. In *Nicholas v. Goord*, all nine plaintiffs were incarcerated felons convicted in New York at the time they brought this lawsuit. They challenged the 1999 version of New York's DNA statute, which required certain classes of convicted felons to provide

³⁸²Note also that the privacy interest at stake belonged to one convicted of a crime. As all the courts that used the balancing test recognized, one convicted of a crime has a diminished expectation of privacy. See, for example, *Jones v. Murray*, 962 F.2d 302, 306–07 (4th Cir. 1992) (“With...arrest comes the loss of at least some, if not all, rights to personal privacy otherwise protected by the Fourth Amendment.”); *Landry v. Attorney General*, 709 N.E.2d at 1094 (“[C]onvicted persons... have a low expectation of privacy in their identity...”).

³⁸³See *Johnson v. Quander*, 440 F.3d 489, 499 (D.C. Cir. 2006) (“Today, however, the DNA Act applies only to felons, and CODIS operates much like an old-fashioned fingerprint database (albeit more efficiently).”).

DNA samples to be maintained in a state database according to N.Y. Exec. Law § 995 *et seq.* (McKinney 1999).³⁸⁴

New York's law is similar to the numerous DNA-indexing statutes that have been established at both the state and federal levels and

1. mandates the extraction of DNA samples from certain classes of convicted felons, according to *id.* § 995-c(3);³⁸⁵
2. provides for DNA information obtained from those samples to be maintained in an index, or database, *id.*;
3. specifies that DNA samples will be analyzed only for markers "having value for law enforcement identification purposes," [656] *id.* § 995-c (5);³⁸⁶
4. allows for release of DNA records only in limited circumstances, *id.* § 995-c (6);³⁸⁷
5. penalizes the unauthorized disclosure or use of DNA records, *id.* § 995-f; and
6. requires that an individual's DNA records be expunged if his conviction is reversed or if he is pardoned, *id.* § 995-c (9).

³⁸⁴ The statute, originally enacted in 1994, at first applied only to individuals convicted after January 1, 1996. 1994 N.Y. Laws, ch. 737, §§ 1, 3. In 1999, the statute was amended to apply to persons already convicted of certain offenses who were still serving a sentence. 1999 N.Y. Laws, ch. 560, § 9. Plaintiffs, all of whom were convicted before 1996 and were serving their sentences in 1999, became subject to the statute at that time. References to the statute throughout this opinion are entirely to the 1999 version. The parties agree that subsequent amendments are not at issue. N.Y. Exec. Law § 995 *et seq.* (McKinney 1999).

³⁸⁵ The 1999 statute applied only to certain felonies (e.g., assault, homicide, rape, incest, escape, attempted murder, kidnapping, arson, burglary). See N.Y. Exec. Law § 995(7).

³⁸⁶ DNA databases like New York's utilize "junk DNA," which does not (as far as we know) contain genetic information. See *United States v. Kincaide*, 379 F.3d 813, 818 (9th Cir.2004) (en banc), *cert. denied*, ___ U.S. ___, 125 S.Ct. 1638, 161 L.Ed.2d 483 (2005).

³⁸⁷ Records may only be released (1) to law-enforcement agencies for identification of specified human remains or for identification purposes in criminal investigations, (2) to a defendant or his legal representative, or (3) after personally identifiable information has been removed, to authorized entities for the purpose of maintaining a population-statistics database. N.Y. Exec. Law § 995-c (6).

All nine plaintiffs provided blood samples for purposes of the DNA index.³⁸⁸

Suing under 42 U.S.C. § 1983, the plaintiffs claimed that New York's statute violates the Fourth Amendment, which prohibits unreasonable searches and seizures.³⁸⁹ They sought to have their DNA records removed from New York's database as well as receive monetary damages.³⁹⁰ In addition to defendants-appellees Goord and Lapp ("State defendants"), plaintiffs named as defendants Medilabs, Inc. and its employee Jessica Walsh, who conducted DNA sampling for the state.³⁹¹

In *Nicholas v. Goord*, the Second Circuit expressed an awareness of the potential for a more significant intrusion on privacy because database samples were kept permanently: "it is potentially a far greater intrusion than the initial extraction of DNA, since the state analyzes DNA for information and maintains DNA records indefinitely."³⁹² The court then concluded that the potential intrusion was unlikely, given

³⁸⁸ Although the statute originally required that DNA be extracted by blood sample, see 1994 N.Y. Laws, ch. 737, § 3, the statute was amended in 1999 to require only "a sample appropriate for DNA testing," 1999 N.Y. Laws, ch. 560, § 3. The state maintains that its "current normal practice . . . is to [obtain DNA by taking] [b]uccal cheek swab[s]," but conceded at oral argument that plaintiffs have all had their blood drawn. We therefore confine our analysis to the extraction of plaintiffs' DNA via blood sample. In any event, even less intrusive measures of obtaining physiological data, such as cheek swabs, can constitute a search, since "[t]he ensuing chemical analysis of the sample" may also effect an "invasion of the [searchee's] privacy interests." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 616, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989).

³⁸⁹ U. S. Const. amend. IV.

³⁹⁰ At the time of filing, two plaintiffs had not yet had their blood drawn; they initially sought to bar the state from doing so. At oral argument, however, the parties informed the court that all nine plaintiffs have had their blood drawn for DNA-indexing purposes. We therefore understand that all plaintiffs now seek the same remedies.

³⁹¹ Private parties are subject to the Fourth Amendment if they act as agents of the state. See *Skinner*, 489 U.S. at 614, 109 S.Ct. 1402; *United States v. Bennett*, 709 F.2d 803, 805 (2d Cir.1983). Under 42 U.S.C. § 1983, private parties acting under color of state law can be held liable for violations of federal constitutional rights. See *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 152, 90 S.Ct. 1598, 26 L.Ed.2d 142 (1970); *Fries v. Barnes*, 618 F.2d 988, 990-91 (2d Cir.1980).

³⁹² 430 F.3d 652, 670 (2d Cir. 2005).

the procedural safeguards of New York's database statute that limited the use of the stored samples.³⁹³

A few genetic-database opinions have begun to outline broader dimensions of genetic privacy. These interpretations discuss a more expanded breadth and depth of the available genetic information and show a preliminary identification of certain key elements in genetic privacy based on its status as more than merely for identification or related informational purposes. Those outlines show multiple aspects of the concept of genetic privacy and implicate DNA analysis beyond the previously defined limited use and comparison to fingerprinting, photographing, and traditional blood testing.

In *Patterson v. State* (2000), an Indiana appellate court found that “at a minimum, it is clear that the results of DNA analysis provide extremely personal information about an individual” even though it upheld the constitutionality of the genetic-database statute.³⁹⁴ In his concurrence in *United States v. Kincaide* (2004), Circuit Court Judge Gould harkened back to Brandeis and Warren's 1890 seminal article on the right to privacy and expressed concern about the potential abuse of information obtained from DNA. He wrote,

In our age in which databases can be “mined” in a millisecond using super-fast computers, in which extensive information can, or potentially could, be gleaned from DNA (even the “junk” DNA currently used), and

³⁹³ 430 F.3d 652, 670 (2d Cir. 2005); see also *State v. Raines*, 857 A.2d 19, 40 n.17 (Md. 2004) (“Although Appellee and the amici speak of doomsday type scenarios where every person's, including non-convicts', DNA would be subject to search by both police and unauthorized persons and soon would be subject to nearly unregulated access, the current version of the Maryland DNA Collection Act does not even approach such unregulated access to DNA profiles.”). Other courts have acknowledged at least the possibility of a broader conception of genetic privacy. *Johnson v. Quander*, 440 F.3d at 499–500 (a *Kyllo* analogy); *Padgett v. Donald*, 401 F.3d 1273, 1281 (11th Cir. 2005) (an analogy to female guards watching naked men); *State ex rel. Juvenile Department v. Orozco*, 878 P.2d 432, 435 (Or. Ct. App. 1994) (recognizing that blood-testing may be a “greater insult to human dignity than fingerprinting”).

³⁹⁴ *Patterson v. State*, 742 N.E.2d 4, 10 n.3 (Ind. Ct. App. 2000).

in which this data can easily be stored and shared by governments and private parties worldwide, the threat of a loss of privacy is real, even if we cannot yet discern the full scope of the problem.³⁹⁵

In a federal district court opinion³⁹⁶ later overturned by the First Circuit, Judge Young articulated a sense of genetic privacy that went beyond the tangible boundaries of information and bodily integrity. He wrote,

Today this Court faces the latest iteration in the growing tension between technology's ability to advance governmental purposes and the Fourth Amendment's protection of individual privacy. This tension is faced and resolved by balancing the government's purpose against the resulting intrusion on the individual. When conducting such a balancing test, the immediate and tangible imperatives of the governmental purpose often outshine and eclipse the more telescopic and inchoate value of personal privacy. The willingness to watch the erosion of such rights silently is most likely where the vanishing liberties are perceived as not our own. It is even more acute where the subjects are those who have derided and evaded, through criminal misconduct, the order and legal structure on which they now rely.³⁹⁷

In an earlier case, also reversed by the First Circuit, Judge Keeton characterized the information obtained in DNA database searches as “immensely private.”³⁹⁸ More dramatically, in his dissent in the *en banc* decision in *United States v. Kincade*, Judge Reinhardt wrote expansively about the core upon which DNA testing intruded:

³⁹⁵ 379 F.3d 813, 842 (9th Cir. 2004) (en banc) (Gould, J., concurring).

³⁹⁶ *Supra* note 269. See generally Wertz et al., *Guidelines on Ethical Issues* (discussing genetic-privacy issues in light of the Human Genome Initiative from the perspective of healthcare professionals); *United States v. Stewart*, 468 F. Supp. 2d 261, 282 (D. Mass. 2007).

³⁹⁷ *United States v. Stewart*, 468 F. Supp. 2d 261, 282 (D. Mass. 2007) (emphasis added), rev'd, 532 F.3d 32 (1st Cir. 2008). The First Circuit did not reject Judge Young's characterization of the privacy interest at stake. It rejected the result of his balancing; 532 F.3d (1st Cir. 2008) at 33–34.

³⁹⁸ *United States v. Weikert*, 421 F. Supp. 2d 259, 269 (D. Mass. 2006), rev'd, 504 F.3d 1 (1st Cir. 2007). The court said, “Not only is the information itself thus immensely private, but the means of storing this information in a centralized database that could potentially be accessed for improper reasons is itself a significant intrusion on privacy interests.” *Ibid*.

Yet the current CODIS database, when it is compared to its modest beginnings, represents an alarming trend whereby the privacy and dignity of our citizens are being whittled away by imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen - a society in which government may intrude into the secret regions of man's life at will.³⁹⁹

The words “more telescopic and inchoate value of personal privacy,” “immensely private,” “privacy and dignity” and “the secret regions of man’s life” seem to refer to additional facets to genetic privacy along with its physical or informational components and one that can be identifiable as dignitary with a privacy dimension. This dimension of dignitary privacy leads to a more intangible sense of violation caused by the repeated intrusion on one’s DNA, something that could potentially occur in genetic databases maintained by private institutions. Taken together, the physical integrity, informational, and dignitary perspectives on privacy revealed by genetic database cases form the core components of a multidimensional portrait of genetic privacy that is worthy of evaluation in cases involving the surreptitious harvesting of out-of-body DNA.

The Protected Core: A Kaleidoscope of Identity

In the case of surreptitious harvesting, the protected core is what some have referred to as “kaleidoscope of identity,” a constantly changing pattern of elements that define a sense of self. This sense is physical in that DNA is within the body or a part of the body—a cell; it is ubiquitously present in every nucleated cell, and it is permanent and relatively immutable. The sense of self is deeply personal and informational, meaning that DNA contains a broad range of medical and other information specific to

³⁹⁹ *United States v. Kincaid*, 379 F.3d at 851 (Reinhardt, J., dissenting) (alterations in original) (emphasis added) (quoting *Osborn v. United States*, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting)).

the individual to whom it belongs. DNA carries information that is personal, predictive, intimate, powerful, shared, and heritable. These qualities are dignitary in that DNA contains information and is so specific and sensitive that, when analyzed by the government, a for-profit company, or a research laboratory, it may reveal more about an individual than he or she might want to know.

In case law and public discourse, DNA is often referred to as a “code,”⁴⁰⁰ “a map,”⁴⁰¹ a “language,”⁴⁰² and a “library,”⁴⁰³ to mention a few. These metaphors for genetic material also suggest a predictive, information-laden sense of identity contained within DNA. One might even broaden those metaphors to refer to DNA as a personal encyclopedia, a repository of personal information that can be consulted repeatedly over time. It forms the core of a person’s identity and separates one person from the other. Applying the kaleidoscope metaphor to describe DNA points toward the multidimensional nature of personal identity that DNA embodies, characteristics of which ultimately define an individual, such as the color of hair and eyes, gender, ethnicity, congenital and susceptible illnesses, age, and lifespan are all encoded in DNA and passed on to progeny. The multidimensional of DNA also implies a multi-faceted quality that is carried within genetic material, assigning a unique identity to an individual. Therefore, one can make an argument that DNA is entitled to physical, informational, and dignitary privacy.

⁴⁰⁰ For example, Kevles and Hood, *The Code of Codes*, 60.

⁴⁰¹ For example, Rothman, *Genetic Maps and Human Imaginations*, 189.

⁴⁰² For example, Collins, *The Language of Life*, 6.

⁴⁰³ For example, Davies, *Cracking the Genome*, 33.

Physical Privacy

The term “physical privacy” encompasses at least three overlapping versions of the term:

1. It can refer to the body or bodily integrity where a person’s body is private to that individual.
2. It can refer to location where the physical location is part and parcel of the individual.
3. It can also refer to a tangible and proprietary quality, meaning that a person’s DNA has unique ownership and, therefore, cannot belong to anybody else.

The language of the Fourth Amendment captures elements of each of these in the following words, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”⁴⁰⁴

The Supreme Court’s basis for rejecting a reasonable expectation of privacy during surreptitious harvesting of DNA as a search tool is that the samples retrieved were outside the suspect’s body. Embedded within the language of courts, one can decipher three versions of physical privacy attributed to a person’s DNA in the following three cases:

1. “When the defendant discarded the straw, he also discarded any expectation of privacy in the DNA evidence on the straw. While it is unlikely that the defendant

⁴⁰⁴ U.S. Const. amend. IV.; *People v. Sigsbee*, No. 03.

believed that he was discarding bodily fluids that would show his DNA profile, nonetheless...”⁴⁰⁵

2. “In any event, we believe the same abandonment analysis applies equally to the items seized or the shed DNA samples obtained from them.”⁴⁰⁶
3. “The relevant question in this case is whether when a person licks an envelope and places it in the mail retains any privacy interest in his saliva at all.”⁴⁰⁷

The notion that Bly had no subjective expectation of privacy is compelled not by a finding that he legally abandoned them as much as it is by his wholesale failure to manifest any expectation of privacy in the items whatsoever.⁴⁰⁸ The Courts ruled based on the reasoning that the DNA was not forcibly taken from inside the individual’s body, that it was voluntarily abandoned, or that it was placed in the mail and sent away from home. This reasoning depends on one’s conception of what is tangible or physically visible, and what is being searched.

If one conceives the search to be of a cup, cigarette butt, saliva, or blood that is outside the body, then DNA’s out-of-body status matters. One does not intrude upon the physical boundary of a body to retrieve abandoned cups, straws, blood or saliva. Most individuals who discard these items do so unknowingly and are, consequently, most probably unaware of any connection to a reasonable expectation of privacy. If one

⁴⁰⁵ *People v. Sigsbee*, No. 03-0342, slip op. at 31–32 (Onondaga, N.Y. Cnty. Ct. Oct. 30, 2003) (emphasis added).

⁴⁰⁶ *State v. Christian*, No. 04-0900, 2006 WL 2419031, at *4 (Iowa Ct. App. Aug. 23, 2006) (emphasis added).

⁴⁰⁷ *State v. Athan*, 158 P.3d 27, 33 (Wash. 2007) (emphasis added).

⁴⁰⁸ *Commonwealth v. Bly*, 862 N.E.2d 341, 357 (Mass. 2007) (emphasis added).

conceives of the point of intrusion as one's DNA and the cells within which the DNA resides as an extension of the body, the argument could change. Now, entry into the physical boundaries of a body takes place when a nucleated cell is lysed to obtain its DNA. In this scenario where the cell is an extension of the human body, there is a reasonable expectation of privacy when cells are collected for DNA isolation and analysis, whether they are abandoned or attached to the physical body.

By itself, the proposal that an entry into out-of-body DNA or an out-of-body cell constitutes an intrusion into the body appears to stretch credulity. It would seem to expand the boundaries of what traditionally constitutes the body beyond that which is either practical or sensible. Yet, such a seemingly novel concept may not be implausible. The *Kyllo v. United States* the Supreme Court found that the search of a location, such as a home, took place even though a house was never entered. Yet, *Kyllo* had a reasonable expectation of privacy when the police measured heat leaving his house.⁴⁰⁹ Drawing parallels between using thermal-imaging technology to discern activity within the home and using forensic DNA technology to discern what is in the body is not necessarily perfect. However, in both situations or circumstances, one can recognize that an intrusion can take place without crossing a traditional physical boundary.

Other physical-privacy cases focusing on the location of the searched item support the notion that neither traditional physical boundaries nor location necessarily resolve the Fourth Amendment issue. In *United States v. Chadwick*, the U.S. Supreme Court analyzed a situation in which the police were legally in possession of a car and

⁴⁰⁹ *Kyllo v. United States*, 533 U.S. 27, 34–36 (2001).

legally inside the car. Therein, they discovered a double-locked trunk.⁴¹⁰ The police removed the trunk from the car, transported it to a federal facility, and then opened it without a warrant, finding marijuana inside.⁴¹¹ The Court held that the police unlawfully opened the trunk without the requisite warrant.⁴¹²

In *California v. Acevedo*, a 1991 follow-up to *United States v. Chadwick*, the police stopped the driver of a car with probable cause because they believed the car contained a bag with marijuana in the trunk.⁴¹³ In effectively overruling *Chadwick*, the United States Supreme Court found, in *Acevedo*, that the police could search the container within the car without a warrant as long as they had probable cause to search that container.⁴¹⁴

Analogous Case Law

The analogy to surreptitious DNA harvesting is direct, although not intuitive, in each of these cases because one can draw parallels between suspect DNA confiscation and each scenario. When the police seized the envelope in *Athan*, they seized the car in *Chadwick* and in *Acevedo*. When they removed the saliva from the envelope in *Athan*, they seized the container in *Chadwick* and in *Acevedo*. When they entered the cell to extract the DNA in *Athan*, they searched the trunk in *Chadwick* and the bag in *Acevedo*.

⁴¹⁰ *United States v. Chadwick*, 433 U.S. 1, 3–4 (1977), abrogated by *California v. Acevedo*, 500 U.S. 565 (1991).

⁴¹¹ *United States v. Chadwick* at 4–5.

⁴¹² *United States v. Chadwick* at 15–16.

⁴¹³ *California v. Acevedo*, 500 U.S. at 567.

⁴¹⁴ *California v. Acevedo*, 500 U.S. at 580–81.

This analogy can also extend to sophisticated technology and instrument confiscations such as mobile phones, laptop computers, iPads, desktop computers, and the like. In cell phone cases, courts have found that a cellphone owner has an expectation of privacy in the contents of the phone.⁴¹⁵ However, this privacy does not hold true at United States border crossings where there is a border search exception. The Supreme Court has consistently held that the Fourth Amendment's “balance of reasonableness is qualitatively different at the international border than in the interior.”⁴¹⁶

In *State v. Smith*, the police arrested Smith and found a cell phone in his possession.⁴¹⁷ The police searched the cell phone and discovered call records and phone numbers of value to their investigation.⁴¹⁸ The Ohio Supreme Court found that Smith had a protected privacy interest in the contents of his cell phone and declined to apply the search incident-to-arrest exception, ruling that the police should have obtained a search warrant prior to seizing Smith’s cellphone and examining the information stored within.⁴¹⁹

In these cases, a direct analogy to surreptitious DNA harvesting can be drawn. For example, when the police seized the envelope in *Athan*, the equivalent to that is the arrest

⁴¹⁵ *United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008); *United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007); *United States v. Quintana*, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009); *United States v. Morales–Ortiz*, 376 F. Supp. 2d 1131, 1139 (D. N.M. 2004); *State v. Boyd*, 992 A.2d 1071, 1075 (Conn. 2010), cert. denied, 131 S. Ct. 1474 (2011). Also see *United States v. Mercado-Nava*, 486 F. Supp. 2d 1271, 1276 (D. Kan. 2007) (“Mere physical possession or control of property is not sufficient to establish standing to object to a search of that property.” (quoting *United States v. Arango*, 912 F.2d 444, 444–46 (10th Cir. 1990))).

⁴¹⁶ See *United States v. Montoya de Hernandez*, 473 U.S. 531, 535 (1985).

⁴¹⁷ *State v. Smith*, 920 N.E.2d 949, 950 (Ohio 2009).

⁴¹⁸ *State v. Smith*, 920 N.E.2d 949, 950 (Ohio 2009).

⁴¹⁹ *State v. Smith*, 920 N.E.2d 955 (Ohio 2009).

of the defendant in *Smith*. Removal of saliva from Athan's envelope corresponds to the seizure of *Smith's* cell phone. When cells from Athan's saliva were used to isolate its cells and extract DNA, it was the equivalent of searching the contents of *Smith's* cellphone. If there is a reasonable expectation of privacy, as the courts found in the warrantless search of *Smith's* trunk, bag, and cell phones, then the DNA obtained from the salivary cells in *Athan* should also have prior probable cause and, by extension, a warrant to search his DNA that was harvested surreptitiously.

These analogies hold only if a reasonable expectation of privacy in one's DNA is merited as much as a reasonable expectation of privacy is afforded in a double-locked trunk (as in *Chadwick*), a bag (as in *Acevedo*), or a cell phone (as in *Smith*). In *Chadwick*, a double-locked trunk implied a proactive sense of security. In *Smith*, it appears that he had placed security measures in his cellphone that prevented easy access to stored information such as phone call records. Surreptitious harvesting implies a search for an inaccessible item and hints that, in such cases, it is associated with the core of a physical being.

Analogous Scientific Testing

In DNA analysis when a suspect's STR profile is examined along with control DNA, the forensic scientist must first isolate DNA from other cellular debris,⁴²⁰ remove any possible inhibitors to the PCR amplification process,⁴²¹ and quantitate and test the

⁴²⁰ Butler, *Forensic DNA Typing*, *supra* note 16, at 42.

⁴²¹ Butler, *Forensic DNA Typing*, 49.

resulting DNA.⁴²² Subsequently, the analyst needs to amplify (i.e., copy) the DNA to a sufficient quantity for further analysis⁴²³ after fluorescent labeling to visualize in an electropherogram.⁴²⁴ The unlocking of the cellular “trunk” or scrolling of the “cellular” phone can also be compared to unlocking sophisticated molecular biological processes in vitro using cell lysing agents, enzymes, thermal cyclers and DNA templates.⁴²⁵

Ironically, as inaccessible as DNA seems, it is in fact ubiquitously present. DNA is present in every nucleated cell in the human body including those that can be inadvertently shed such as skin, bodily fluids, hair follicles, and growing ends of nails.⁴²⁶ Thus, the “item” for surreptitious-harvesting searches is part of the physical core of every living being. DNA exists in all nucleated cells, and even in cell-free blood extracts, and represents the starting point of life in many species. It would follow that without the presence of DNA, advanced life forms, as one knows today, would not exist.⁴²⁷

Analogous Fingerprints

The analogy of traditional fingerprint obtained at the scene of a crime presents an interesting contrast to DNA fingerprinting from abandoned genetic material. Although an

⁴²² Butler, *Forensic DNA Typing*, 50.

⁴²³ Butler, *Forensic DNA Typing*, 63.

⁴²⁴ Butler, *Forensic DNA Typing*, 330.

⁴²⁵ See generally Butler, *Forensic DNA Typing* (explaining the process of forensic DNA typing as applied to criminal forensics).

⁴²⁶ National Research Council, “DNA Technology in Forensic Science,” *supra* note 9, at 17, 34.

⁴²⁷ Contrast this kind of search to the one in *Schmerber v. California*, 384 U.S. 757, 758 (1966), where the police, via a physician, obtained a blood sample from a DUI suspect, or to the one in *Winston v. Lee*, 470 U.S. 753, 756 (1985), where the police, via a surgeon, sought to surgically remove a bullet from the body of an attempted robbery suspect.

identifying feature like DNA, fingerprints by themselves are neither inaccessible nor situated inside a cell or the body, unlike DNA. They can be accessed from the surface, albeit from a specific place on the body. A forensic scientist must be trained appropriately, paying careful attention to detail to develop a fingerprint when taken from an individual or obtained from a crime scene.⁴²⁸ However, the technological sophistication required to obtain a fingerprint is less than that required for forensic DNA analysis. Although ubiquitously present, human hands are not as inaccessible as DNA.

This argument alone does not resolve the fingerprint and DNA comparison. It is common knowledge among forensic scientists that both fingerprints and DNA are important resources to crime solving by providing unique identification to an individual. But, one resource is much more easily accessible than the other. Fingerprints can be lifted without involving cellular isolation and its penetration. They also do not provide the degree of personal information that DNA analysis is capable of revealing about a person.

The most important quality shared by fingerprinting and DNA analysis is that both reveal identifying information accurately. Much of the identifying powers and value of both fingerprints and forensic DNA analysis is from the nature of the information that is derived from careful study and applying said information to the case. However, there are also differences between fingerprinting and DNA analysis in terms of accessibility, methodology, and quality of information that can be obtained.

The physical location of fingerprints makes it easy to access them. They are present at the tip each human finger and everyone has characteristic and unique

⁴²⁸ See generally Cole, *Suspect Identities: A History* (explaining the complexity of the fingerprint identification process).

fingerprint patterns, a useful tool of identification when a photograph is unavailable.

Fingerprints are valuable for identification purposes because

1. they contain information from the tips of fingers: an accessible, common, permanent feature in every person, and
2. that information is “unique”, distinguishing one individual from another.⁴²⁹

These features make fingerprinting a powerful and useful identification tool.

However, accessing a person’s DNA requires greater effort if it is not willingly provided.

A physical sample must be collected with the hope that at least a single intact cell is present on the item. The cell must be carefully entered using sophisticated technology to isolate the DNA. The DNA must be amplified with PCR for multiple cycles using primers directed to the thirteen or more chosen loci used for STR analysis. The products (i.e., suspect DNA and crime scene DNA) must be separated alongside control and experimental samples to compare and determine whether the DNA found at the crime scene matches that of the suspect. One must also hope that there was no cross contamination and that the tests were performed with utmost care and results analyzed with great precision.

Therefore, differences between fingerprinting technology and DNA technology chiefly reside in three areas.

1. Location: differences in accessibility, physical location
2. Methodology: isolation methods vary significantly
3. Quality of information: DNA can predict farther into the future than fingerprints.

⁴²⁹ Placing recent litigation surrounding fingerprints aside, see, for example, *Commonwealth v. Patterson*, 840 N.E.2d 12, 26–28 (Mass. 2005) (comparing the degrees to which different fingerprinting analysis techniques reliably identify an individual).

Informational Privacy

Informational privacy with respect to DNA is one of the most significant considerations for genetic privacy. Information obtained from DNA analysis can be intimate, personal, shared with relatives, predictive, and therefore, powerful. DNA analysis can potentially capture a composite view of data valuable not only to the police, but also to genealogists seeking to profit from this information. The informational privacy dimension of DNA has been the primary focus of the genetic-database case law on genetic privacy. Although every court has declined to act based on the informational-privacy features of DNA,⁴³⁰ many of them have conceded its importance and highlighted its potential in dissenting or concurring comments. The classic description of DNA's informational value is Judge Reinhardt's dissent in *United States v. Kincade*:

What type of information might the government eventually be able to extract from samples of junk DNA? Even today, as the plurality admits, "DNA profiles derived by STR may yield probabilistic evidence of the contributor's race or sex." Yet that seems to be a dramatic understatement. The DNA "fingerprint" entered into CODIS likely has the potential to reveal information about an individual's "genetic defects, predispositions to diseases, and perhaps even sexual orientation." DNA analysis can reveal the presence of traits for thousands of known diseases, and countless numbers of diseases which are currently unknown. More ominously, some have predicted that the DNA profiles entered into CODIS will someday be able to predict the likelihood that a given individual will engage in certain types of criminal, or non-criminal but perhaps socially disfavored, behavior.⁴³¹

⁴³⁰ The courts have arrived at this conclusion because (1) the information obtained for inclusion in a genetic database is alphanumeric and one-dimensional and (2) the use of that limited information is strictly controlled by statute. See, for example, *Nicholas v. Goord*, 430 F.3d 652, 668 (2d Cir 2005) (observing that "junk DNA" serves no known purpose other than to establish identity); *State v. Raines*, 857 A.2d 19, 33 (Md. 2004) (dismissing fears of "unregulated access to DNA profile[s]"); *State v. Martin*, 955 A.2d 1144, 1155 (Vt. 2008) (noting that database indexes genes "not associated with any known physical trait"); *State v. Athan*, 158 P.3d 27, 34 (Wash. 2007) (acknowledging potential for privacy violations with DNA information). In the surreptitious-harvesting circumstance, neither the state nor the federal government appears to regulate the information obtained.

⁴³¹ *United States v. Kincade*, 379 F.3d 813, 850 (9th Cir. 2004) (en banc) (Reinhardt, J., dissenting) (citations within not included).

In his dissent in *Rise v. Oregon*, Judge Nelson also highlighted the especially sensitive nature of the information in DNA: “DNA genetic pattern analysis catalogs uniquely private genetic facts about the individual that should be subject to rigorous confidentiality requirements even broader than the protection of an individual’s medical records.”⁴³² In *United States v. Weikert*, Judge Keeton further characterized a genetic database as one in which “the files that are kept for perpetuity are replete with information the scope of which science has not yet discovered.”⁴³³ Therefore, the case law alludes to DNA possessing

1. information about congenital or acquired genetic mutations, predispositions to diseases, possibly sexual orientation, the presence of traits for thousands of known diseases, and diseases which are currently unknown;
2. predictive information about certain types of antisocial or noncriminal but socially unacceptable behavior; and
3. more generally, uniquely private genetic information that is greater than that available in medical records.

Predictive Information

DNA is organized into regions called Open Reading Frames (ORFs) that encode proteins and in non-coding DNA sequences which make up the majority of the three

⁴³² 59 F.3d 1556, 1569 (9th Cir. 1995) (Nelson, J., dissenting), abrogated by *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), and *Ferguson v. City of Charleston*, 532 U.S. 67 (2001).

⁴³³ *United States v. Weikert*, 421 F. Supp. 2d 259, 269 (D. Mass. 2006), rev’d, 504 F.3d 1 (1st Cir. 2007).

billion base pairs of DNA that humans have in each diploid cell.⁴³⁴ Mutations in specific places in a single or multiple ORFs could increase the susceptibility to long term illnesses or lingering diseases that are potentially terminal, requiring costly medical care.⁴³⁵

Therefore, information obtained from DNA can be also categorized as predictive.

The nature of genetic information is predictive and has a probabilistic component. Genetic disorders are controlled by a defective single gene that causes disease.⁴³⁶ Much of the information obtained from genetic studies indicates that it can predict the occurrence of a disease. For example, the variants of the “breast cancer gene” that have been identified as cancer causing can only inform carriers that such a variant increases the likelihood of developing breast cancer by a certain percentage or probability over the course of someone’s lifetime when compared to someone who does not carry the mutant gene in the general population.⁴³⁷

Predictive genetic information can be of several types and with varying degrees of certainty. Newspapers frequently publish the discovery of a novel gene that correlates with a medical condition, disorder, trait, or a behavior.⁴³⁸ For example, scientists have

⁴³⁵ Springer Nature, “Open Reading Frames,” at <https://www.nature.com/subjects/open-reading-frames>.

⁴³⁶ See Mutations and Disease at <https://genetics.thetech.org/about-genetics/mutations-and-disease>. “But the mutations we hear about most often are the ones that cause disease. Some well-known inherited genetic disorders include cystic fibrosis, sickle cell anemia, Tay-Sachs disease, phenylketonuria and color-blindness, among many others. All of these disorders are caused by the mutation of a single gene.”

⁴³⁶ National Health Service National Genetics Education and Development Center, *Single Gene Disorder*. A notable exception is Huntington’s disease. National Center for Biotechnology Information, *Huntington’s Disease*.

⁴³⁷ National Cancer Institute, *BRCA1 and BRCA2: Cancer Risk*.

⁴³⁸ See generally Kaplan and Rogers, *Gene Worship: Moving Beyond* (critiquing the frequent genetic explanations for human behavior).

identified genes associated with obesity,⁴³⁹ risk-taking,⁴⁴⁰ smoking,⁴⁴¹ creativity,⁴⁴² schizophrenia,⁴⁴³ impulsivity, and violence.⁴⁴⁴

Biotechnology companies exist to identify disease causing mutant genes and to determine the probability of manifestation. One such company is deCODE Genetics, which advertises diagnostic tests for a variety of genetic conditions on its website, including tests for obesity, common forms of breast cancer, prostate cancer, glaucoma, elevated cholesterol, hypertension, and cardiac risk.⁴⁴⁵ Its most comprehensive test is a personal genetic scan, deCODEme, that “analyses genetic risk factors for 48 diseases ranging from heart attack and diabetes to lung cancer and traits like ABO blood types, eye color and male pattern baldness.”⁴⁴⁶

Other companies like 23andMe offer genealogy and ancestry services that are all the contemporary rage among consumers seeking personalized genetics and a revelation of their ethnic or biogeographic ancestry background.⁴⁴⁷ Genetic information about physical traits or conditions can be reliable. Forensic tests for the color of eyes and hair and other traits continue to be developed in an effort to provide investigators with a more

⁴³⁹ Herbert et al., “A Common Genetic Variant,” 279.

⁴⁴⁰ Lin et al., “The Dosage of the NeuroD2,” 14877, 14879.

⁴⁴¹ Malayandi et al., “Impact of CYP2A6 Genotype,” 400.

⁴⁴² Bachner-Melman et al., “AVPR1a and SLC6A4 Gene Polymorphisms,” 394.

⁴⁴³ Vacic et al., “Duplications of the Neuropeptide,” 499.

⁴⁴⁴ Meyer-Lindenberg et al., “Neural Mechanisms of Genetic Risk.”

⁴⁴⁵ deCODE GENETICS, <http://www.decode.com/products/> (last visited Aug. 17, 2011).

⁴⁴⁶ deCODE GENETICS.

⁴⁴⁷ 23andMe, <http://www.23andme.com/>. 23andMe uses the catch phrase, “Genetics just got personal.”

composite physical portrait of a potential suspect drawn from a crime scene sample.⁴⁴⁸ In terms of informational privacy predictive genetic information provides a glimpse into an individual's present and future. George Annas has eloquently labeled genetic information a "future diary" that "informs our younger selves about our aging selves."⁴⁴⁹

Shared Information

Genetic information is also shared information that is passed on from parent to offspring. Because genetic information is hereditary, the DNA of blood relatives is more similar than that of the unrelated population. For example, with paternity testing, laboratories compare the DNA of a putative parent with a child to determine possible parentage.⁴⁵⁰ One begins to know to whom one is biologically related when one is in possession of an individual's DNA. As noted in the introduction of this thesis, this proposition has formed the basis for the activities of amateur genealogists, divorce lawyers, and DNA paparazzi.⁴⁵¹

Prosecutors have also begun to use genetic information obtained from DNA analysis more creatively. Based on the work of Mark Shriver and others, tests exist to discern biogeographical information from DNA—testing that can identify the continent

⁴⁴⁸ Frudakis, *Molecular Photofitting: Predicting Ancestry*, 613.

⁴⁴⁹ It is in code and probabilistic, but just as private. It is information about *you*, information about which you should have a right *not* to know, a right to say, "I don't want to know this." But even if you want to know it, you should have a right to say, "I don't want anybody else to know it. I don't want my employer to know it. I don't want the FBI to know it. I don't want my school to know it. I don't want my colleagues to know it. I don't want my spouse to know it. I don't want my children to know it." It should be your choice.... [I]n terms of information, I believe that our DNA resembles a future diary that is due the same privacy that we afford other written diaries. Annas, "Genetic Privacy: There Ought," 9, 11.

⁴⁵⁰ National Research Council, *The Evaluation of Forensic DNA Evidence*, 53–54.

⁴⁵¹ See *supra* notes 8–9 and accompanying text. See generally Rothstein, "Genetic Stalking and Voyeurism," 539 (discussing uses and publication of genetic information and recommending legislation).

of origin, ethnic background, or race of the individual.⁴⁵² A serial murder case in Louisiana changed course based on biogeographical testing data that directed the police to a non-Caucasian suspect rather than a Caucasian suspect who was initially being pursued.⁴⁵³ In this case, investigators shifted their focus away from white suspects after an analysis of tissue from one of the crime scenes determined that the killer was probably black.

Due to erroneous FBI offender profile and inaccurate eyewitness accounts, Louisiana police originally believed the killer to be white and tested the DNA of thousands of Caucasian men in and around the general area of the murders. The tests did not yield a suspect and without any leads, police allowed a company named DNAPrint Genomics to access DNA from the crime scenes. DNAPrint Genomics generated an ancestry profile indicating that the suspect was 85% African, thus changing the course of the investigation.⁴⁵⁴

Between the DNA evidence gathered from deceased victims, ancestry evidence of the suspect, a psychological profile made by a victim named Mary Ellen O'Toole, and a police sketch based on another victim's description, the police went public with the information.⁴⁵⁵ Police in nearby Zachary, Louisiana, recognized the suspect from a recent peeping tom incident that they had recently investigated. Police in Zachary shared the suspect's name along with his DNA sample with the police in Baton Rouge,

⁴⁵² Frudakis, *Molecular Photofitting: Predicting Ancestry*, *supra* note 113, 35–145.

⁴⁵³ Wade, "Unusual Use of DNA" A28.

⁴⁵⁴ Touchette, "Genome Test Nets Suspected Serial Killer," at http://www.genomenetwork.org/articles/06_03/serial.shtml

⁴⁵⁵ *State v. Lee*, 964 So. 2nd 967 (2007).

Louisiana. When the DNA lab ran and compared the suspect's samples, they were found to be a perfect match to Derrick Todd Lee.⁴⁵⁶

Once Derrick Todd Lee was identified as the primary suspect in these crimes, law enforcement located and captured him in Atlanta, Georgia. Lee was returned to Baton Rouge, where he was tried in August 2004 for the murder of GERALYN DeSoto, who had been found dead in her home in Addis, having been stabbed numerous times. DNA evidence that linked Lee to the crime had been discovered. Although Lee was eligible for first degree murder charges, the District Attorney elected to try Lee for murder in the second degree because DeSoto had not been sexually assaulted, which meant a first-degree murder conviction would be difficult to obtain. Lee was convicted by jury and sentenced to life imprisonment without parole.⁴⁵⁷ This dramatic change in investigation appears to be the first of its kind where DNA was used to extract details of a criminal suspect's appearance, according to the developer of the genetic test. Shriver, a geneticist at Pennsylvania State University, developed of the test used in Louisiana.⁴⁵⁸

Although DNA evidence has come into widespread use to identify individuals, the pieces of DNA that are identifying markers are not part of the genome that reveal a person's physical makeup. Experts in forensic genetics have known that as knowledge of the human genome advances, other information could be extracted from DNA samples, including physical traits like race. Shriver said he had identified markers that are specific units or short sequences of DNA, which are more often found in people from one

⁴⁵⁶ *State v. Lee*, 964 So. 2nd 967 (2007).

⁴⁵⁷ *State v. Lee*, 964 So. 2nd 967 (2007).

⁴⁵⁸ *Supra* note 333 Wade, "Unusual Use of DNA," A28.

continent than another. If enough markers are used, a researcher can say with reasonably high confidence to which of the major continental races such as African, Caucasian, East Asian or American Indian that a person belongs, as well as the percentage of each ancestry in the case of people of mixed race.⁴⁵⁹

Investigators sent DNA samples taken from the crime scene to DNAPrint Genomics, a company in Sarasota, Florida, that owns the rights to Shriver's test. Of twenty samples tested, only one was linked to the suspect and the company was not told which sample was taken from the crime scene. It typed the crime scene sample as being eighty-five percent African ancestry and fifteen percent American Indian.

As far as cases where other physical characteristics were concerned, Dr. Duceman said, "This is the first that I'm aware of." Conversely, Dr. Mark Batzer, a population geneticist at Louisiana State University, where the Louisiana serial killer's last victim was a graduate student, said, "My prediction is that the test will become more utilized." Shriver, the inventor of the race identifying genetic test said that investigators had been searching for a white man, based on profiling information suggesting that most serial killers are white. The suspect arrested in the case, Derrick T. Lee, is black. Dr Shriver said he did not know whether Mr. Lee had any Indians among his ancestors.⁴⁶⁰

More recently, police and prosecutors have utilized a powerful technique known as familial searching, a procedure that grew out of the compilation of state and federal databases testing the previously mentioned thirteen-loci genetic information on incarcerated convicts or suspected in ongoing criminal cases. The police submit the

⁴⁵⁹ Wade, "Unusual Use of DNA," A28.

⁴⁶⁰ *Supra* note 333.

thirteen-loci genetic profile of the crime scene sample of unknown origin into the CODIS database.⁴⁶¹ If no direct match is found, laboratories that perform familial searching then rank order the top 50-150 offender samples based on the likelihood of them being derived from a first degree relative (parent, child, sibling) of the crime scene DNA profile.⁴⁶² Then, typically Y-chromosome STR testing is performed and if a Y-STR match is found, this suggests that the individual who contributed the crime scene sample is closely related to the offender in the CODIS database.⁴⁶³ After close verification of results, the laboratory then turns over the single name of the offender to the detectives who then proceed with their investigation to determine which of the possible relatives of the offender may be a viable suspect. Once other data are assembled, a clandestine DNA sample may be obtained, or one from a warrant, to obtain a sample for STR comparison to the crime scene evidence.⁴⁶⁴

These examples confirm that genetic information from DNA not only reveals details of physical attributes but also to whom the person in question is related and to what biogeographical/ancestral groups they belong. Genetic information is such that it can be shared by more than just one person, distinguishing their physical qualities and racial profile.

⁴⁶¹ Epstein, “‘Genetic Surveillance’—The Bogeyman Response,” 141, 145.

⁴⁶² Epstein, “‘Genetic Surveillance’—The Bogeyman Response,” 146.

⁴⁶³ Epstein, “‘Genetic Surveillance’—The Bogeyman Response,”

⁴⁶⁴ Epstein, “‘Genetic Surveillance’—The Bogeyman Response,” 145–146.

Personal and Intimate Information

Because it contains both predictive and shared information, DNA information is also personal and intimate. DNA also carries information about a person's current and possible future medical conditions that the individual might otherwise choose not to disclose. Therein lies the basis for fine tuning future laws that states may choose to pass to protect genetic privacy. Strikingly, someone in possession of others' DNA would have access to sensitive information that can be regarded as deeply personal and even not in their own knowledge. In other words, the person in possession of the DNA could obtain information about other people that they do not know about themselves.

Other situations may arise where in a legal custody battle between two family members, a genetic counselor becomes aware that the couple's child only has a genetic relationship to one and not both parents. The personal and intimate nature of such information in the hands of a third party can be misused. In the context of Fourth Amendment genetic privacy, the third party with that knowledge would be the government, defense attorney or another family member. One can also envision a situation where the third party could be a genealogy data firm.⁴⁶⁵

Powerful Information

The predictive, shared, personal, and intimate nature of genetic information also makes it a powerful tool for misuse. To address the possibility of misuse, preemptive measures have been placed by proactive legislators. A variety of laws have been passed

⁴⁶⁵ It is critical, once again, to recognize in this discussion of what is genetic privacy that the focus is on the individuals' *expectation* of privacy in their DNA, not on their level of certainty as to whether the government has or would access such information or what the government would do with such information if it had or did access the information.

to curtail potential abuse by employers, co-workers, identity stealers, and third parties that would sell or purchase the information without the owner's consent. Most states now have genetic antidiscrimination laws in the area of health insurance so that consumers do not face any bias from insurance firms.⁴⁶⁶ Several states have such laws addressing the employment context,⁴⁶⁷ and genetic privacy laws are quite common.⁴⁶⁸

Historically, there is documented evidence of misuse of even pseudo-genetic information in the United States. The eugenics era, which was in the first part of the twentieth century, is a vivid and painful historical reminder of abuses that occurred from the misapplication of genetic information. Hundreds of thousands of individuals were sterilized based on pseudo-genetic information.⁴⁶⁹ Carrie Buck, a subject of the notorious *Buck v. Bell* case upholding the constitutionality of involuntary sterilization,⁴⁷⁰ was committed to the Virginia Colony for Epileptics and Feeble-minded, in Lynchburg, VA, and involuntarily sterilized because Carrie, her mother, and her daughter were believed to be "feeble-minded," and this was considered to be a hereditary condition.⁴⁷¹ In *Buck v. Bell*, Oliver Wendell Holmes stated

We have seen more than once that the public welfare may call upon the best citizens for their lives. It would be strange if it could not call upon

⁴⁶⁶ Kass, "The Implications of Genetic Testing" 312–13.

⁴⁶⁷ Rothstein, "The Law of Medical," *supra* note 158, at 281, 291–93. See generally Allen, "Genetic Privacy: Emerging Concepts" 31 (discussing various definitions of "genetic privacy" and the legal and ethical values of each).

⁴⁶⁸ For example, N.H. REV. STAT. ANN. § 141-H ("[N]o individual . . . shall be required to undergo genetic testing as a condition of doing business with another person.").

⁴⁶⁹ See Kevles, *In the Name of Eugenics*, 100 (discussing introduction of sterilization laws in the United States).

⁴⁷⁰ *Buck v. Bell*, 274 U.S. 200, 207 (1927).

⁴⁷¹ Kevles, *In the Name of Eugenics*, *supra* note 127, at 110–11.

those who already sap the strength of the State for these lesser sacrifices, often not felt to be such by those concerned, in order to prevent our being swamped with incompetence. It is better for all the world if, instead of waiting to execute degenerate offspring for crime or to let them starve for their imbecility, society can prevent those who are manifestly unfit from continuing their kind. . . . *Three generations of imbeciles are enough.*⁴⁷²

The scope of eugenic legislation went beyond involuntary sterilization statutes. More than twenty-five states revised their respective marriage laws to prevent the “biological continuation” of the unfit.⁴⁷³ Immigration restrictions were passed that used “IQ” tests to restrict immigration, particularly of Eastern and Southern Europeans.⁴⁷⁴

The multi-dimensional informational quality of DNA contrasts sharply with the unidimensional quality of the information of fingerprints.⁴⁷⁵ Fingerprint information is unique and unshared, where no two people have the same fingerprints. Like forensic DNA information, fingerprints can identify the source of a crime scene sample and are a potent investigative tool when available. Like DNA, fingerprints can identify a person, but beyond serving as a source of identification, fingerprints have no determined predictive value to date. Unlike DNA, the information obtained from fingerprinting is neither intimate nor personal in nature.

The informational basis for making an argument to include a reasonable expectation of genetic privacy among those granted by the Fourth Amendment is twofold. First, DNA is a dynamic entity with a potential for giving life and altering the course of an individual’s life. The information encoded in DNA strands may hold the key

⁴⁷² *Buck v. Bell*, 274 U.S. 200, 207 (1927).

⁴⁷³ *Buck v. Bell*, 274 U.S. 200, 99–100.

⁴⁷⁴ *Buck v. Bell*, 274 U.S. 200, 94–95.

⁴⁷⁵ Interestingly, while fingerprints can be obliterated to some extent by physical mutilation, DNA cannot, thereby lending it an informational permanence akin to its physical permanence.

to one's birth, existence, and death. DNA has information that makes each person unique, relates people to others, and allows parents to pass characteristics on to progeny. In doing so, it is vital to continuing life as one knows it. Second, advances in cloning technology have now made it possible to duplicate another being with available DNA. The entire process can be successfully performed in a laboratory, without the need for human reproduction.

DNA is spatially and temporally dynamic. Its physical and informational presence emphasizes the kaleidoscopic nature of the identifying features it possesses. A piece of DNA does not exist in isolation as a self-sufficient entity. Oftentimes, one region of DNA influences another, at times across great distances within the chromosomal organization to produce "an effect" or outcome. For example, some cancers involve the mutation of genes which, unmutated, would suppress the unregulated growth of certain cells whose normal function is itself regulated by other genes.⁴⁷⁶

More broadly, as sequencing of human genomes intensified, scientists have become increasingly aware of the dynamism within the human genome, even in regions of DNA thought to be dormant or considered junk DNA. The ENCODE Project Consortium has begun looking at non-gene regions of DNA and has concluded that "through the analysis of 1% of the human genome that the humble, unpretentious non-gene sequences have essential regulatory roles."⁴⁷⁷ Multi-factorial disorders that have

⁴⁷⁶ See Mukherjee, *The Emperor of All Maladies*, 368–69 (discussing how the lack of "negative" genes leads to the formation of cancer cells).

⁴⁷⁷ Greally, *Encyclopedia of Humble DNA*, 447 (discussing The Encode Project Consortium, *Identification and Analysis of Functional Elements in 1% of the Human Genome by the ENCODE Pilot Project*, 447 NATURE 799 (2007)). The regions the consortium studied had previously been known as regions containing "junk" DNA—DNA of no known use. See Kolata, "Bits of Mystery DNA," (noting that DNA studied by ENCODE Project was previously considered "junk" DNA). As Greally entertainingly explains: "The results of the pilot phase of this project, which involved an analysis of 1% (30 megabases)

genetic, behavioral, and environmental roots seem to be more prevalent than Mendelian genetic disorders.

The interplay between genes, environment, and behavior is the hallmark of multifactorial disorders, such as some types of cancer, asthma,⁴⁷⁸ and diabetes.⁴⁷⁹ Interactions between one's genes, the physical environment within or outside one's body, or with the consequences of one's behavior may cause genes to be turned off or on or to take a different pathway of expression. The recent understanding that many complex disorders have, among other things, genetic roots stands at the beginning of a much more profound scientific understanding of such disorders as asthma, atherosclerosis, diabetes, hypertension, and obesity.⁴⁸⁰ It already explains how profoundly DNA is intertwined in a layered, dynamic process refracting through time and space to create portions of who we are, physically and informationally. Thus, DNA is a multi-faceted, multi-generational with a multilayered identity.

of the human genome, are not good news for genes, which will no longer be able to hog the limelight. Even this preliminary study reveals that the genome is much more than a mere vehicle for genes, and sheds light on the extensive molecular decision-making that takes place before a gene is expressed." Greally, *supra*, at 783.

⁴⁷⁸ See generally Martinez, "Genes, Environments, Development and Asthma" 179 (studying interactions between genetic determinants for asthma and their genetic, environmental, and developmental contexts).

⁴⁷⁹ See generally Riserus et al., "Dietary Fats and Prevention" 44 (studying the effect of dietary fat on the risk of type 2 diabetes).

⁴⁸⁰ See Korstanje and Paigen, "From QTL to Gene," 235 *passim* (discussing the technique of mapping QTL genes, which identifies chromosomal regions affecting various illnesses, and asserting that "the harvest of QTL genes is just beginning").

Dignitary Privacy

Dignitary privacy is contemplative of an intangible concept of what privacy means and is not driven by the obvious physical and informational aspects of privacy. All conceptions of privacy in some respect refer to an intrusion upon a protected core. For some of these conceptions, the protected core is, primarily, something relatively concrete—a body, a place, an object, or even information.⁴⁸¹ In Solove’s delineation of the traditional expressions of the idea of privacy, these conceptions of privacy would include limited access to the self, secrecy, and the control of personal information.⁴⁸² Other conceptions that are evocative of more intangible measures of privacy—one’s identity, sense of self, and dignity. Now, the meaning of a protected core has an absence of physicality and materialism. Rather, it becomes primarily intuitive.

In the language of Solove’s traditional expressions, it is the right to be let alone, to personhood, and to intimacy.⁴⁸³ These features of the protected core do not exist independent of more concrete ones. But they capture an aspect of that core that contributes to building on the ideals of their concrete siblings. For example, when a home is burglarized, the homeowner has suffered an intrusion on several very tangible aspects of a protected core—the home, items that were taken, and perhaps information to which the burglar had access. The homeowner also has suffered an intrusion on a more intangible aspect of that core—the sense that an unwanted person has been within a zone that is personal and intimate. The second intrusion, to some extent, builds on the first

⁴⁸¹ Solove, *Understanding Privacy*, *supra* note, at 12–13.

⁴⁸² Solove, *Understanding Privacy*, *supra* note, at 12–13.

⁴⁸³ Solove, *Understanding Privacy*, *supra* note, at 12–13.

because no intrusion on the intangible core would occur without the more concrete intrusion on home, property, and information. However, more has occurred than just physical intrusion.

When we hear friends or family describing a burglary of their residence, often, they say: “It’s not what they took; it’s the sense that someone was in my house.” Or, “It’s creepy to think someone was here.” It may go too far to suggest in this context that the intangible violation goes to the core of who one is or one’s dignity. These expressions seem independent of physical intrusion. Instead, they speak to the notion of feeling violated in a personal space that goes above and beyond that which one can grasp physically. Part of the challenge is that physical intrusion is easier to explain and for others to comprehend, whereas an assault on a person’s dignity is difficult to convey harder to quantify. Societal expectations are geared toward understanding material losses rather than those associated with emotion or the feeling of well-being. For these reasons, it is challenging to make others comprehend its true value.

Surreptitious harvesting of out-of-body DNA realigns the calculus of privacy values. Currently, most courts view the physical intrusion as nonexistent and the informational intrusion as limited at least in its use. Though the victim of governmental surreptitious harvesting feels no physical pain, the presence of the government “in her DNA” and the knowledge of that presence are intrusions on one’s dignity and self-identity. In genetic-database cases in which judges spoke of “[t]he more telescopic and inchoate value of personal privacy”; of DNA being “immensely private”; of “privacy and dignity”; and of “the secret regions of man’s life.”⁴⁸⁴ To have the government present in

⁴⁸⁴ See *supra* notes 165-167 and accompanying text. See 165 *United States v. Stewart*, 468 F. Supp. 2d 261, 282 (D. Mass. 2007) (emphasis added), *rev’d*, 532 F.3d 32 (1st Cir. 2008). The First Circuit

one's DNA and to have the government store one's DNA without any limits on its use speaks of a limit on individual autonomy. That presence and that storage, undisclosed as it may seem, might affect one's conduct and self-identity. And, this effect might occur even though the government may never actively do anything with the DNA.

The dignity inherent in individual autonomy free of governmental interference flows from one's inherent dignity as a human being—what many call a “negative liberty.”⁴⁸⁵ The idea of dignity as a constitutional consideration is common. Noemi Rao has written that the concept of inherent dignity is present in much of the Supreme Court's constitutional jurisprudence. For example, as the Court has addressed issues of drug testing, self-representation, sexual autonomy, reproductive rights, and free speech, it has discerned the concept of inherent dignity in the First, Fourth, Sixth, and Fourteenth Amendments.⁴⁸⁶ In *Planned Parenthood of Southeastern Pennsylvania v. Casey*, the plurality said:

These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. *At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life.* Beliefs about these matters could not define the attributes of personhood where they formed under compulsion of the State.⁴⁸⁷

did not reject Judge Young's characterization of the privacy interest at stake. It rejected the result of his balancing. 532F.3d (1st Cir. 2008) at 33–34; *United States v. Weikert*, 421 F. Supp. 2d 259, 269 (D. Mass. 2006), *rev'd*, 504 F.3d 1(1st Cir. 2007). The court said: “Not only is the information itself thus immensely private, but the means of storing this information in a centralized database that could potentially be accessed for improper reasons is itself a significant intrusion on privacy interests.” *Ibid.* *United States v. Kincade*, 379 F.3d at 851 (Reinhardt, J., dissenting) (alterations in original) (emphasis added) (quoting *Osborn v. United States*, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting)).

⁴⁸⁵ Rao, “Three Concepts of Dignity,” 183, 203–05. Much of what follows draws on Rao's analysis of the three kinds of dignity that constitutions protect.

⁴⁸⁶ Rao, “Three Concepts of Dignity,” 207–16.

⁴⁸⁷ 505 U.S. 833, 851 (1992) (emphasis added).

In *Miranda v. Arizona*, the U.S. Supreme Court was also emphatic about the role of dignity in its analysis of the Fifth Amendment right against self-incrimination when it spoke of “one overriding thought: the constitutional foundation underlying the privilege is the respect a government—state or federal—must accord to the dignity and integrity of its citizens.”⁴⁸⁸ More specifically, the idea of dignitary privacy is central to the Fourth Amendment. It is the most explicit privacy amendment to the Constitution, and, over the years, the United States Supreme Court has consistently identified dignity as one of the interests protected by the Fourth Amendment from a case like *Schmerber v. California* (the Fourth Amendment protects personal privacy and dignity where the United States Supreme Court held that intrusions to the human body require a warrant)⁴⁸⁹ to a case like *City of Ontario, California v. Quon* (the Fourth Amendment guarantees privacy, dignity, and security).⁴⁹⁰

The idea of dignitary privacy also appears in circumstances involving newer technology. Conceptually, the GPS tracking and the public video surveillance examples seem to represent practical circumstances that raise dignitary, as well as other, privacy concerns. In the GPS cases, most commonly, the police place a GPS device on the outside of a suspect’s car while it is in a public place in order to track the travels of the car’s driver.⁴⁹¹ The police did not engage in any physical intrusion, either in the suspect’s

⁴⁸⁸ *Miranda v. Arizona*, 384 U.S. 436, 460 (1966) (emphasis added).

⁴⁸⁹ 384 U.S. 757, 767 (1966).

⁴⁹⁰ 130 S. Ct. 2619, 2627 (2010).

⁴⁹¹ *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (tracking suspect’s whereabouts via GPS constitutes search for Fourth Amendment purposes); *United States v. Moran*, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) (attaching a GPS device to defendant’s vehicle did not constitute search or seizure);

car or on his or her property, in order to access the car. In the public video surveillance circumstance, the police positioned cameras in strategic locations to film all the activity and people involved there.⁴⁹² Again, in capturing people's faces and conduct as they go about their daily business, the police intrude neither on their bodies nor on any physical zone of privacy.

In both circumstances, the privacy intrusion is one that essentially occurs in public. It is to a protected core that relates to one's presence in the public world. One can conceive of this core in a number of ways beyond simply the gathering of personal or intimate information: Does one NOT have the right to be left alone, even in public?⁴⁹³ Does one NOT have a right to anonymity even when in public?⁴⁹⁴ Does one NOT have the right not to be always watched by the government?

This less tangible, more dignitary sense of privacy is, at best, an emerging one in the GPS cases. In *State v. Jackson*, a 2003 GPS case, the Washington Supreme Court recognized a very substantial informational-privacy interest against 24-hour GPS surveillance.⁴⁹⁵ In doing so, it also noted with approval the analysis of the Oregon Supreme Court in a radio-transmitter case. In the case, the court evaluated a kind of

Osburn v. State, 44 P.3d 523, 526 (Nev. 2002) (suspect "had neither a subjective nor an objective expectation of privacy in the bumper of his vehicle"); *State v. Jackson*, 76 P.3d 217, 224 (Wash. 2003) ("[C]itizens of this State have a right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle, regardless of reduced privacy expectations due to advances in technology.").

⁴⁹² See Slobogin, "Public Privacy: Camera Surveillance" 213, 219–22 (describing the use of surveillance cameras in the United States); Slobogin, *Privacy at Risk*, 82–83 (same).

⁴⁹³ See generally Warren and Brandeis, "The Right to Privacy," 193 (describing the right to be left alone).

⁴⁹⁴ Slobogin, *Privacy at Risk*, at 79–117.

⁴⁹⁵ *State v. Jackson*, 76 P.3d, 224 (Wash. 2003).

privacy interest on top of the already significant informational one it had found: The court reasoned that use of a device that enabled the police to locate a person within a 40-mile radius day or night “is a significant limitation on freedom from scrutiny” and “a staggering limitation upon personal freedom.” The court noted that allowing use of such radio transmitters would mean that “individuals must more readily assume that they are the objects of government scrutiny” noting that commentators “have observed that *freedom may be impaired as much, if not more so, by the threat of scrutiny as by the fact of scrutiny.*”⁴⁹⁶

Yet, in *United States v. Jones*, a case involving surreptitious GPS surveillance, the Supreme Court did not explicitly describe the privacy interest at stake.⁴⁹⁷ And the public-video surveillance cases have not yet made their way into the case law in the United States.⁴⁹⁸ Whatever the current level of recognition of a dignitary-privacy invasion in the GPS-tracking cases, the above examples show that the focal point of a dignitary-privacy claim is the presence of an “other” as the scrutinizer. Whether the scrutiny accompanies a bodily invasion (*Schmerber*), a cell phone (*Quon*), one’s decision making (*Casey*), or one’s psyche (*Miranda*), it is the fact that someone else is there, that one is not alone, or that the other is uninvited that is the essence of the violation.

⁴⁹⁶ *State v. Jackson*, 76 P.3d, at 224 (emphasis added) (quoting *State v. Campbell*, 759 P.2d 1040, 1048 (Or. 1988)).

⁴⁹⁷ The plurality focused narrowly on a property analysis, one that a group of four justices felt resolved the issue. See 132 S. Ct. at 949–53. Justices Sotomayor’s and Alito’s opinions at least explored the informational-privacy dimension of the practice. See *Ibid.*, at 957 (Sotomayor, J., concurring) (arguing for right of privacy information); *Ibid.*, at 964 (Alito, J., dissenting) (concluding that the public has an expectation of privacy in GPS tracking data).

⁴⁹⁸ Public-video-surveillance usage is much more developed in England. See Slobogin, *Privacy at Risk*, *supra* note 276, at 83–84 (discussing the extent of surveillance in the United Kingdom).

The sense of violation that accompanies the dignitary intrusion does not grow merely out of the other's physical presence or the other's active interference with one's body or one's personal information. To paraphrase and extend the logic of one court, freedom may be impaired as much, if not more so, by the thought that someone has been there, is there, or may be there, whether they did, said, or took anything.⁴⁹⁹ Or, as Justice Sotomayor noted in her *Jones* concurrence, "[a]wareness that the Government may be watching chills associational and expressive freedoms."⁵⁰⁰ To be scrutinized in and of itself offends one's dignity whatever the use to which the scrutiny is put.

The nature of a Fourth Amendment dignitary-privacy invasion requires that a governmental authority engage in the scrutiny. The idea that the government in some capacity is present in one's decision-making, one's cell-phone conversations, one's psyche, or one's daily whereabouts accentuates the harm to one's dignity.⁵⁰¹ Anthony Amsterdam directly addressed the fundamental issue in his 1974 piece on *Katz* and the Fourth Amendment:

The ultimate question, plainly, is a value judgment. It is whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society. That, in outright terms, is the judgment underlying the Supreme Court's decision in *Katz*, and it seems to me the judgment that the Fourth Amendment inevitably requires the Court to make.⁵⁰²

⁴⁹⁹ *State v. Campbell*, 759 P.2d at 1048.

⁵⁰⁰ 132 S. Ct. at 956.

⁵⁰¹ Decision-making and psyche invasions like those in *Casey* and *Miranda* occur under the Fifth and Fourteenth Amendments. Nonetheless, the specter of the governmental presence is the same.

⁵⁰² Amsterdam, "Perspectives on the Fourth Amendment," 349, 403.

What offends one's dignity is that scrutiny of DNA offers up the kaleidoscope of identity to those with access. The dignitary intrusion is not what the government will or may do with such access. It is that the government gets to look into the kaleidoscope in all its layered, temporal, and spatial richness. The mere presence of the government at that window on core identity is the dignitary intrusion,⁵⁰³ and it compounds the physical and informational intrusion. In contrast, the dignitary intrusion associated with fingerprinting is less significant. Fingerprints, too, represent a color in the identity spectrum. Like DNA, fingerprints are in code and are available in public. Unlike DNA, they are less biologically locked, and the quality of their identifying information is relatively one-dimensional in contrast to DNA's kaleidoscope of identity. Superficial by nature, fingerprints do not give rise to a sense that they provide a window on core identity. Thus, while a mild dignitary invasion may exist when the government possesses fingerprints, it is not as much in depth when compared to invasion associated with DNA fingerprinting and corroborated by societal views.⁵⁰⁴

Any assessment of the expectation of privacy that people have in DNA will be an approximation that inevitably includes a measure of subjective judgment. This is because the concept of harming one's dignity implies a level of definitional certainty and objectivity that is anything but the case. Dignity is, by its nature, a very subjective concept—one person's dignity may be another's pain and suffering. Historically, it has

⁵⁰³ This dignitary intrusion is exacerbated because some police departments have begun compiling DNA databases of samples collected in circumstances outside those covered by the regulatory structures of state and federal law. For example, the New York City medical examiner's office purportedly has a "linkage" or "rogue" database that includes former suspects, arrestees, and others never convicted of a crime. See Willing, "Authorities Find More Uses."

⁵⁰⁴ See discussion in "Societal Perspectives in Genetic Privacy" below.

been a moving target mostly, particularly as a legal concept.⁵⁰⁵ Including an assessment of the extent of dignitary harm in measuring one's expectation of privacy risks reduces the assessment to merely one individual's judgment. The *Katz* test accounts for this concern. It requires a subjective expectation of privacy and an expectation of privacy that society is willing to recognize as reasonable.⁵⁰⁶ The objective focus of the second prong moderates the risk of the test offering Fourth Amendment protection to over personalized, idiosyncratic senses of privacy. The challenge then is to lend at least some empirical meaning to the genetic privacy that "society is prepared to recognize as reasonable,"⁵⁰⁷ to do so in a way that transcends the idiosyncratic, the personal, and the anecdotal and to avoid mere theorizing.

Societal Perspectives on Genetic Privacy

The U.S. Supreme Court has periodically sought societal views on a reasonable expectation of privacy and its protection outside the traditional Fourth Amendment model. In *Rakas v. Illinois*, the Court expressed an interest in external legal concepts, like property law and in "understandings that are recognized and permitted by society"⁵⁰⁸ and

⁵⁰⁵ Neomi Rao captures this slipperiness well: As a fundamental precept of human rights and basic liberties, dignity really took hold after the Universal Declaration of Human Rights stated "All human beings are born free and equal in dignity and rights." But even in the Universal Declaration, the start of international efforts to protect human dignity, the drafters disagreed about the meaning of human dignity. Today, widespread adoption of dignity in modern constitutions and human rights documents has not led to any greater consensus—rather different conceptions of dignity remain. The fact that "dignity" is an important yet slippery concept has become commonplace. Rao, "Three Concepts of Dignity," *supra* note 159, at 185–86 (footnotes omitted).

⁵⁰⁶ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

⁵⁰⁷ *Katz v. United States*, 389 U.S. 347, 361 (1967) (internal quotation marks omitted).

⁵⁰⁸ *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978); see also Slobogin and Schumacher, "Reasonable Expectations of Privacy" 727, 731 ("Although this language appeared in a footnote, and was directed solely toward defining the standing concept, it has since been relied upon in the text of several

that idea has continued to appear in the Court's jurisprudence.⁵⁰⁹ Christopher Lobefin and Joseph Schumacher have also made effort towards empirically quantifying the public's understanding of a variety of Fourth Amendment privacy interests. In 1993, Slobogin and Schumacher surveyed over 200 people "to ascertain their understanding of these interests implicated in several police investigative techniques."⁵¹⁰ From the survey, Slobogin and Schumacher developed the preliminary hypothesis that court decisions about where expectations of privacy lie do not necessarily reflect societal understandings and, in fact, "tend to underestimate the privacy and autonomy interests infringed on by police actions."⁵¹¹ However, although their study remains unique to date, Slobogin and Schumacher conducted their survey at a time when the police were not utilizing either genetic databases or surreptitious DNA harvesting to solve cases.

Other Fourth Amendment scholars have not extended this empirical approach to more current kinds of police investigative efforts. Some polling does exist on the general idea of genetic privacy, addressing questions on genetic information and genetic discrimination.⁵¹² One such study surveyed 1,199 individuals about their level of trust in doctors, spouses, researchers, law enforcement, health insurers, and employers with access to test results for genetic disorders.⁵¹³ At the extreme, 86% had some or a lot of

other cases involving the 'search' issue, often rephrased in terms of expectations of privacy 'society is prepared to recognize as reasonable.'").

⁵⁰⁹ Slobogin and Schumacher, "Reasonable Expectations of Privacy," 731-32.

⁵¹⁰ Slobogin and Schumacher, "Reasonable Expectations of Privacy," 732.

⁵¹¹ Slobogin and Schumacher, "Reasonable Expectations of Privacy," 732.

⁵¹² See, for example, Apse et al., "Perceptions of Genetic Discrimination," 511 (studying people's fears over genetic discrimination).

⁵¹³ Genetics and Public Policy Center, *U.S. Public Opinion*, 1-2, available at <http://www.dnapolicy.org/policy.polls.htm>

trust in their doctors, whereas only 16% had some or a lot of trust in their employers.⁵¹⁴

Law enforcement fell in the low middle with 46% of respondents expressing some or a lot of trust and 54% expressing only a little or no trust.⁵¹⁵

Without results from direct surveys conducted on surreptitious DNA harvesting or on privacy concerns related to police possession of genetic information, an examination of the use of DNA in public culture helps to understand fundamental attitudes about DNA. A sampling of 30 individuals was conducted informally to determine if DNA privacy was an important issue to them. Participants in the survey represented the U.S. population from its two most populated areas, the North East and California. The raw data from this survey are presented in Appendix A.

Print Media

Another resource of public view on genetic privacy comes from the media and the context in which they have discussed or portrayed DNA to their readership. Albert E. Scherr at University of New Hampshire School of Law examined how the term “DNA” was used over a period of one year in two well-known US-based newspapers, the *New York Times* and *USA Today*.⁵¹⁶ The study was conducted to examine societal attitudes toward DNA and whether that was informative in making a determination about genetic

⁵¹⁴ Genetics and Public Policy Center, *U.S. Public Opinion*, 2.

⁵¹⁵ Genetics and Public Policy Center, *U.S. Public Opinion*, 2.

⁵¹⁶ Scherr, "Genetic Privacy and the Fourth Amendment," 517-518. Scherr and colleagues recorded every mention of DNA over a one-year period in both newspapers. The papers were selected because both have a national circulation and arguably different and possibly with overlapping readerships. Scherr found that although the term was used by journalists, the premise underlying this study is that journalists would use of DNA or its metaphors that would be within their audience's comprehension to explain something that is less understood at a scientific level.

privacy. The *New York Times* had 267 mentions of DNA over the course of the year, and 73.8% of them were scientific references, not metaphorical ones. In *USA Today*, 63.9% of the 180 references were scientific. In both newspapers, the significant majority of its uses were as a scientific term referencing genetic research or forensics rather than as a metaphor. Interestingly, just about one-quarter of the *New York Times* references and over one-third of the *USA Today* references were metaphorical.⁵¹⁷

News articles where DNA was used metaphorically were primarily of three areas: Sports, Business, and the Arts. In *USA Today*, the metaphorical use of DNA occurred most frequently in sports articles, followed closely by business articles, and to a lesser extent, in articles related to the arts including television.⁵¹⁸ In the *New York Times*, the use of DNA occurred most frequently in business articles, followed by the arts and to a lesser extent, in sports related articles.⁵¹⁹ In articles about business, it was the behavior of a company;⁵²⁰ in articles about music or the arts, it was the behavior of a band,⁵²¹ an artist,⁵²² or an author; and in articles about sports, it was an individual's⁵²³ or a team's⁵²⁴ behavior.

⁵¹⁷ Out of 267 references in the *New York Times*, 197 were scientific and 70 were metaphorical. In *USA Today*, 115 references were scientific and 65 were metaphorical.

⁵¹⁸ Of the 65 references in *USA Today*, DNA was used metaphorically 22 times in sports articles, 18 times in business/marketing articles, and 10 times in arts articles. There was lesser use in political articles (5), book reviews (3), and personal articles (2).

⁵¹⁹ Of the 70 metaphorical uses of DNA in the *New York Times*, 20 occurred in business/marketing articles, 19 occurred in arts articles, and 9 uses occurred in sports articles.

⁵²⁰ See, for example, Bunkley, "Dutch Car Maker Still," at <http://www.nytimes.com/> (addressing Saab's DNA).

⁵²¹ See, for example, Caramanica, "Dapper, Privileged and Unapologetic," at <http://www.nytimes.com/> (traces of ska in Vampire Weekend's DNA).

⁵²² See, for example, Holden, "Three Loners on a Road," at <http://www.nytimes.com/> (character not in actor's DNA).

⁵²³ See, for example, “Peyton Manning Not Looking,” at <http://www.usatoday.com/> (Manning’s preparation in his DNA).

⁵²⁴ Over 90% of the metaphorical uses of DNA in *USA Today* and the *New York Times* involved behavior of some sort as the target domain. See, for example, Dodd, “Why Can’t Cubs Win?” at <http://www.usatoday.com/> (Cubs’ championship-prohibiting DNA).

Chapter IV.

Discussion and Conclusion

Discussion

The need for granting sole proprietorship of DNA to its rightful owner is strengthened when we consider the volume of personal information that it carries and its potential for use. Given the recent pace of advances in forensic DNA technology and unregulated collection of DNA by virtually anyone,⁵²⁵ let alone law enforcement, a backdoor, population-wide data bank is possible, unbeknownst to the population at large. This type of information banking and sharing could become as rapid and widespread as personal information such as someone's address, phone number, visuals of homes, and school and personal records that we may not have officially granted permission to reveal and are now public information, nevertheless. We can change several features of personal identification such as name, passport, address and bank records. With surgical procedures, we can also modify our physical features and the color of hair and eyes; however, our DNA will continue to remain constant and part of our lifelong identity.

Without proper legislation, unregulated collection and banking of that personal information and the risk of discriminatory treatment and possible harassment are possible. Regardless of how discreet the collection might be, law enforcement may

⁵²⁵ Currently, CODIS permits the banking of DNA profiles from persons who have been "convicted of crimes," "charged in an indictment or information with a crime," or "whose DNA samples are collected under applicable legal authorities...." 42 U.S.C. § 14132(1) (2000). At first glance, this third category might appear to cover abandoned DNA collection but given that the statute is explicit in excluding those who have been arrested but not charged and those who voluntarily submit DNA "solely for elimination purposes" abandoned DNA would possibly count among the excluded categories.

collect DNA from virtually anybody, and companies may share it with collaborators for any number of reasons, including drug design and development. Once collected, there is little chance that someone's DNA will be returned or its use regulated. As the anthropologist Pamela Sankar observes, "[o]nce DNA samples exist, it is difficult to restrain their use."⁵²⁶

Once the abandoned DNA is collected, what should happen to the sample? To what uses could the sample be put? The answer to the second question almost certainly will depend on the direction that science evolves, but the answer to the first requires some law and policy decisions in an area already fraught with ambiguity. First, once the police lawfully collect DNA for one investigation, the Fourth Amendment permits reanalysis of that sample for a wholly separate investigation.⁵²⁷ At least one lower court has decided that any further DNA analysis on a tissue sample already obtained for investigating a separate crime does not constitute a search, even if the initial collection of the tissue implicated the defendants Fourth Amendment rights.⁵²⁸ Thus, assuming its collection is

⁵²⁶ Sankar, "DNA-Typing: Galton's Eugenic," 273, 289.

⁵²⁷ Because courts are not likely to deem the collection of abandoned DNA a Fourth Amendment search and seizure, the recent Supreme Court cases scrutinizing the programmatic purpose of searches without suspicion under "special needs" analysis is inapplicable here. The Court's most recent statements in this area include *Illinois v. Lidster*, 540 U.S. 419 (2004) (upholding a highway checkpoint designed to question citizens of a recent crime), *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000) (invalidating a roadside checkpoint designed to discover illegal drug activity), and *Ferguson v. City of Charleston*, 532 U.S. 67 (2001) (invalidating a public hospital's nonconsensual drug testing of pregnant patients).

⁵²⁸ See *People v. Baylor*, 118 Cal. Rptr. 2d 518, 521 (Ct. App. 2002) (observing that "there is no constitutional violation or infringement of privacy when the police in one case use a DNA profile, which was lawfully obtained in connection with another case."); *State v. Hauge*, 79 P.3d 131, 144 (Haw. 2003) (noting that "a number of jurisdictions have held . . . that once a blood sample and DNA profile is lawfully procured from a defendant, no privacy interest persists in either the sample or the profile."); *Patterson v. State*, 742 N.E.2d 4, 11 (Ind. Ct. App. 2000) (holding that while initial DNA sampling and analysis taken from defendant constituted a search, "the reuse of his validly obtained DNA sample in a subsequent unrelated criminal investigation did not trigger Fourth Amendment protections."); *Wilson v. State*, 752 A.2d 1250, 1272 (Md. Ct. Spec. App. 1999) (. "Once an individual's fingerprints and/or his blood sample for DNA testing are in lawful police possession, that individual is no more immune from being caught by the DNA sample he leaves on the body of his rape victim than he is from being caught by the fingerprint he

constitutionally proper, a sample of DNA collected after abandonment can be analyzed as many times as the police wish. Second, the Fourth Amendment does not appear to restrict the initial collection of discarded DNA for any reason. Current uses of surreptitiously collected DNA suggest that the police seek a suspect's DNA only to match it against DNA evidence found at a crime scene, but this limitation is generated by the police themselves and not supervised by another entity that enforces restricted use. Little oversight exists regarding the intentional or accidental inclusion⁵²⁹ of such DNA evidence into CODIS, regardless of whether a positive match is made between the collected sample and existing forensic evidence.⁵³⁰ Neither do state laws appear to clearly address how police ought to treat these tissue samples and DNA profiles in relation to state databanks.⁵³¹ Taken together, the Fourth Amendment fails to protect citizens from

leaves on the window of the burglarized house or the steering wheel of the stolen car. . . . No new Fourth Amendment intrusion is involved.”).

⁵²⁹ Federal law itself restricts the use of DNA records contained within CODIS, but it is not obvious why such restrictions would apply to abandoned DNA, which is not addressed directly by the statute, nor by any of the state statutes. See 42 U.S.C. § 14132(b)(3) (limiting disclosure of DNA analysis to “law enforcement identification purposes,” in “judicial proceedings,” “for criminal defense purposes.” And “for a population statistics database.” on an anonymous basis). The American Society for Law, Medicine and Ethics publishes a valuable fifty-state survey of DNA database laws. See also Axelrad, *Survey of State DNA*, at www.aslme.org/dna-04/grid.index.php. Fourth Amendment challenges by inmates and parolees to the forced contribution of their DNA for the federal criminal DNA database, CODIS, have been consistently rejected by state and federal courts. See, e.g., *United States v. Kincaide*, 379 F.3d 813, 830.–31 (9th Cir. 2004) (citing representative cases).

⁵³⁰ Rather than a single centralized source, CODIS is a three-tiered structure of information sharing. All profiles originate from local laboratories (“LDIS”). The states then collect this information for their state-wide databases (“SDIS”). As the highest level of this hierarchy, CODIS is the National DNA Index System (“NDIS”) and permits states participating in the CODIS program to compare samples at a national level. All fifty states, the federal government, Puerto Rico, and the U.S. Army participate at the national level. To aid in criminal investigation, CODIS has two indices: one containing DNA profiles of individuals, and the other containing unidentified DNA from crime scenes. See *The FBI's Combined DNA*, at <http://www.fbi.gov/hq/lab/codis/brochure.pdf>; see also *NDIS Participants*, at <http://www.fbi.gov/hq/lab/codis/partstates.htm>.

⁵³¹ This relates to the larger problem of storing and controlling access to collected DNA samples and accompanying text. See Hibbert, “DNA Databanks: Law Enforcement’s,” 767, 796 (“Although many statutes make it a crime to misuse information in the databank itself, the [DNA] samples, which contain an unlimited amount of information about the offender, receive little, if any protection. . .”). Indeed, the FBI

having their identities—including their sensitive genetic information—revealed through the collection and analysis of discarded or voluntarily given DNA. Under this rubric, “identification” itself proves to be a variable concept.

Courts often note, for instance, that convicted persons lose their legitimate expectations of privacy in their identity.⁵³² But what are the boundaries of “identity” in a world of genetic analysis? Of course, fingerprints themselves, by linking a biometric identifier to a name, provide a window into that person’s past, vis-à-vis his or her criminal history.⁵³³ By linking a tissue sample to a criminal history and to personal medical information, a DNA profile looks both forward and backward in time.

An emerging field in molecular genetics uses DNA information from groups, initially classified by race, to correlate multiple genetic differences among the groups and to test the group’s responsiveness to drug treatments.⁵³⁴ In February 2005, Perlegen Sciences announced it had constructed such a genetic diversity map and more recently, Parabon Nanolabs has also developed a genetic diversity tree.⁵³⁵ One troubling byproduct of this research, as sociologist Troy Duster argues, is the mistaken presumption that a

encourages the states to *retain* portions of the evidence samples from which the analysis is taken. See FBI, *Standards for Forensic DNA*, at <http://www.fbi.gov/hq/lab/codis/forensic.htm> (requiring with Standard 7.2 that “[w]here possible, the laboratory shall retain . . . a portion of the evidence sample or extract.”).

⁵³² See, e.g., *United States v. Kincade*, 379 F.2d 813, 837 (9th Cir. 2004) (noting that once convicted of a felony an offender’s identity becomes a matter of “state interest.”).

⁵³³ It was once hoped that fingerprints would reveal as much as DNA does. In the late nineteenth century, Francis Galton studied fingerprints for hereditary details and hoped to use that information to foster a program of preventing marriages in order “to reverse the alleged degeneration of the English population. . .” See Sankar at 274; see also Kimmelman, “Risking Ethical Insolvency,” 209 (contending that properties of DNA “qualitatively distinguish DNA samples and profiles from fingerprints and militate against convenient analogies to fingerprints.”).

⁵³⁴ Guterman, “Scientists Reveal Map,” at <https://www.chronicle.com/article/Scientists-Reveal-Map-of-Human/120653>; see also National Public Radio, *All Things Considered: Drafting a Genetic Map of Human Diversity* at <http://www.npr.org/templates/story/story.php?storyId=4503527>.

⁵³⁵ See Guterman, *supra* note 10 and Parabon Nanolabs at <https://parabon-nanolabs.com/>.

genetic basis for race actually exists.⁵³⁶ The possibility of a racial genetic map renders it “not at all unreasonable” to expect a project proposing to identify race-based genetic variation among sex offenders or violent felons.⁵³⁷ Such an ability would permit the criminal law not only to be reactive, but predictive, by identifying would-be offenders on the basis of their genetic make-up. Not only can DNA provide nearly undisputable evidence of identity, it may one day be used to identify and isolate those who possess a “crime gene”. The possibility of finding genetic causes for antisocial behavior is the most widely publicized research of “behavioral genetics.”⁵³⁸

Recently, using genetic information for racial and ethnic profiling has come to fore with the news that Chinese government officials have been utilizing forensic DNA technology, scientific know-how, and reagents and testing equipment that were developed in the United States to determine Uighur ancestry.⁵³⁹ Uighurs, who are predominantly Muslim and accused of perpetuating terrorism in China, largely reside in Xinjiang, a region located in the Northwest. Under the guise of providing free health care, Chinese authorities have been taking their DNA without the consent of Uighurs or a

⁵³⁶ See Duster, “Race and Reification,” 1050-1051. As Duster observes, racial groups are used by scientists as one category of variability for reasons of convenience because cell and tissue repositories categorize their own samples by race. Genetic variability, however, can be found between any two categories of groups. See also Guterman, *supra* note 108. Guterman quotes Duster as saying, “If you took a group of people from the East Coast and the West Coast...you’d find differences.... You wouldn’t conclude there were genetic differences between the two coasts. But with race or ethnicity, people are preprogrammed at a cognitive level to think in terms of these genetic categories....” *Ibid*.

⁵³⁷ See Duster, “Race and Reification,” *supra* note 12, at 1051.

⁵³⁸ Nelkin, “Behavioral Genetics and Dismantling,” 156, 158.

⁵³⁹ Regalado, “How US Experts Helped China,” at <https://www.technologyreview.com/f/613000/how-us-experts-helped-china-build-a-dna-surveillance-state/>.

providing means of legal recourse.⁵⁴⁰ Subsequently, Chinese scientists working for the government have documented their findings in a scholarly article and patented their technique that has the ability to differentiate people based in their race such as “Uighurs from Indians.” This campaign of “surveillance and oppression” has also met with outrage and condemnation by United States Senator Marco Rubio. The Massachusetts-based company named Thermo Fisher announced that they will no longer sell their equipment to the Chinese government. However, the *New York Times* claims that Thermo Fisher made that decision only after the newspaper’s scrutiny over its sales to China.⁵⁴¹

By taking advantage of publicly available DNA databases in the United States and contributing Uighur DNA, the Chinese government has breached scientific ethical conduct. It has detained up to a million people in what China calls “re-education” camps, drawing condemnation from human rights groups and a threat of sanctions from the Trump administration. The DNA database that will be generated by the Chinese government is meant to track down and, subsequently, coerce the Uighurs into conforming their government instead of rising in rebellion.⁵⁴² While these actions might be unthinkable or face consequences in Western democracies, they can be realities in parts of the world where personal privacy let alone genetic privacy are not honored and hence face no retribution.

In 1992, the National Institutes of Health funded a controversial conference to discuss the genetic basis of criminal behavior to find a causal relationship between crime

⁵⁴⁰ Wee, “China Uses DNA to Track,” at <https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html>.

⁵⁴¹ *Supra* note 415.

⁵⁴² *Supra* note 415.

and genetics.⁵⁴³ The discovery of such a gene⁵⁴⁴ could provide justifications for profiling, even if it is not racially biased, of preventive detentions or other means of social control for those identified as genetically predisposed to criminality, should that information ever be leaked to those in positions of responsibility.⁵⁴⁵ Even if this seems like a farfetched notion today, should markers be identified for mental illness⁵⁴⁶ or aggression and anti-social behavior,⁵⁴⁷ those behavioral characteristics associated with a propensity for

⁵⁴³ Organizers cancelled the 1992 conference after public objections from African American community leaders, but it was reorganized successfully in 1995 at the University of Maryland as “The Meaning and Significance of Research on Genetics and Criminal Behavior.” See Roush, “Conflict Marks Crime Conference,” 1808–09.

⁵⁴⁴ See, e.g., Lehrman, “Prisoners’ DNA Database Ruled,” 818 (citing Massachusetts state senator James Jajuga for the suggestion that DNA databanks might “yield a ‘criminal.’ DNA profile that could help predict which parolees or probationers were likely to commit further crimes, and identify how to use education, drug therapy or counseling as preventive measures.”).

⁵⁴⁵ See Andrews, “Predicting and Punishing Antisocial Acts,” *supra* note 101, at 116, 117; see also Nelkin, “Behavioral Genetics and Dismantling,” *supra* note 101, at 160 (“Given the pressures of cost and time that currently plague the criminal justice system, genetic explanations of violent behavior conveniently fit with current ideologies about prison reform.”). And, as Troy Duster has pointed out, the search for genetic explanations for differences in human behavior, such as intelligence and mental illness—a search reaching back to nineteenth-century eugenics arguments—can serve political and ideological interests. Genetic explanations hold the potential to identify (and stigmatize) a genetic “underclass.” See generally, Duster, “Backdoor to Eugenics.”

⁵⁴⁶ More than a decade ago, the Congressional Office of Technology Assessment, an agency tasked with providing Congress with analyses on scientific and technological issues, raised this very concern. One report warned that “the possibility exists to test DNA acquired specifically for identification purposes for disease information in a database” and that “[t]his option may become more attractive over time, especially as the number and types of probes for genetic disorders increase.” See Office of Tech Assessment, *Genetic Witness: Forensic Uses*, 132, at <http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk2/1990/9021/902107.PDF> (comparing property and tort law treatments of corpses).

⁵⁴⁷ The prospect of linking DNA to criminal behavior is no different from the early twentieth century hope, however surprising to a contemporary audience, that fingerprints would indicate the same information. In his history of fingerprinting, Simon Cole observes that all criminal identification techniques, in order to become widely accepted, must at least “gesture” toward three claims: (1) that they can identify an individual criminal (“forensic identification”); (2) that they can help create a criminal record of recidivism (“archival identification”); and (3) that they can yield clues that would someday eradicate criminality itself by revealing the biological predisposition to crime (“diagnostic identification”). See Cole, *Suspect Identities: A History*, at 305. DNA analysis, like fingerprinting, offers such promises; Marx, *supra* note 51, at 326 (“Identities are becoming relatively less unitary, homogenous, fixed and enduring, as the modernist idea of being able to choose who we are continues to expand, along with globalization processes and increased integration.”).

criminal conduct,⁵⁴⁸ more expansive DNA analysis would justifiably serve crime control purposes and tagging individuals.

The very idea of sequencing the human genome was unthinkable a generation ago, but the recent completion of the Human Genome Project means that sequencing of an individual's genome is possible, if desired.⁵⁴⁹ After having retrieved abandoned DNA, could the government sequence your genes?⁵⁵⁰ Would private gene banks create “designer” babies through a combination of established in vitro fertilization and cloning techniques for financially well off consumers who want a child with cherry picked physical attributes and intellectual capabilities, qualities sought as desirable in an offspring? Technology—not the Fourth Amendment—could provide the main obstacle.

If such projection sounds like an unthinkable possibility, historical experience has proven how “function creep” has altered and expanded the uses of other information originally meant for identification purposes. The Social Security number is the most prominent example of an identifier now used for purposes not originally intended.⁵⁵¹

⁵⁴⁸ See Imwinkelried and Kaye, “DNA Typing: Emerging,” 413. The authors conclude, contrary to the suggestions made here, that “the better course is to treat human cells left in public places like fingerprints in deciding what expectation of privacy is reasonable.” *Ibid.*, at 440. Kimmelman, “Risking Ethical Insolvency,” 209 (2000) (contending that properties of DNA “qualitatively distinguish DNA samples and profiles from fingerprints and militate against convenient analogies to fingerprints.”).

⁵⁴⁹ Completed in 2003, the Human Genome Project was an international effort to determine the sequence of the base pairs making up human DNA and to identify the approximately 35,000 genes in human DNA. For further information on the Human Genome Project, see ORNL.org, Human Genome Project Information, http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml.

⁵⁵⁰ Because they are not “state actors,” private individuals are not restricted by the Fourth Amendment. But should we restrict them by other means? To demonstrate what they see as the futility of protection against private action, Kaye and Smith ask, “If I am struck by an automobile on a public street and bleed on the crosswalk, then does that mean that I can prevent everyone else from taking a few drops or demand that the blood be returned by the street sweeper who wipes it up?” See Kaye and Smith, “DNA Identification Databases: Legality,” 436 (citing representative case).

⁵⁵¹ Petti, “An Argument for the Implementation,” 703, 726–27 (describing expanding uses of Social Security numbers).

Although it was originally intended to solely track the contributions of working Americans to help calculate retirement benefits, the Social Security number has become substitute for a national identity card today.⁵⁵² Even fingerprinting, the dominant method of criminal identification in the twentieth century, was originally intended as a system of recordkeeping for civil, not criminal, purposes.⁵⁵³

Moreover, DNA collection already has experienced its own function creep. When the U.S. military began collecting mandatory DNA samples from soldiers in 1992, the Department of Defense announced that the use of the samples would be restricted to the identification of dead or injured soldiers.⁵⁵⁴ By 1996, proposals had already been made to extend the use of these samples for medical research.⁵⁵⁵ Today, all blood samples collected from United States military persons tried and convicted by the military are included in the national database, CODIS; however, DNA has not been extracted from the millions of blood spot cards collected from members of the military that are housed at Dover Air Force Base in Delaware as they are only used for identification purposes on an as-needed basis.⁵⁵⁶ While the compulsory collection of DNA samples from prisoners and

⁵⁵² See Office of Tech Assessment, *Genetic Witness: Forensic Uses*, at 115 (describing the Social Security number as “de facto national identifier.” although its current uses “were certainly not anticipated when the social security system was devised.”).

⁵⁵³ The idea of fingerprinting as a system of recordkeeping can be attributed to two men working in two separate fields. In the 1850s, William Herschel proposed first handprints and then fingerprints as a method of recordkeeping over colonial subjects in British India. In 1880, Henry Faulds proposed to the journal *Nature* that fingerprinting might be used to identify criminals. Francis Galton later developed a system of classifying fingerprints, and it was adopted by the British in the early twentieth century over the Bertillonage system of bodily measurements. See Cole, *Suspect Identities: A History*, 60-96.

⁵⁵⁴ See Nelkin and Andrews, “DNA Identification and Surveillance,” 689, 691.

⁵⁵⁵ See Sankar, “DNA-Typing: Galton’s Eugenic,” 287-288.

⁵⁵⁶ See *supra* note 6 about CODIS.

parolees for state and federal DNA databases has continued,⁵⁵⁷ little attention has been paid to this backdoor method of DNA collection.⁵⁵⁸

While there may be little public objection to including convicted offenders and arrestees for DNA data banking, the public may feel quite differently when it is their DNA that is subject to systematic collection.⁵⁵⁹ Reports of pervasive resistance to the most recent census questionnaire and to proposals for national identification cards after the September, 11, 2001, terrorist attacks, for example, suggest widely felt concerns about the government's collection of personal information from ordinary citizens.⁵⁶⁰ Even if public resistance exists towards the practice, law enforcement officers now need

⁵⁵⁷ Today DNA samples from suspects are matched against DNA profiles collected in CODIS, which was established by the federal government but is supplied with samples from both the federal government and the states. See 42 U.S.C. § 14132 (2000).

⁵⁵⁸ Existing discussions of abandoned DNA are largely brief citations of it as a phenomenon to watch. See, e.g., Curley and Caperna, "The Brave New World," 22, 27 (noting that with regard to "abandoned DNA," "the law may need to address previously unthought of privacy concerns."). The most extensive discussion of the issue thus far has been presented by Imwinkelried and Kaye, "DNA Typing: Emerging," 436-440, who identify "abandoned DNA." as one of many "emerging or neglected." issues in legal analysis of DNA sampling. See, e.g., *United States v. Kincaid*, 379 F.3d 813, 836.-39 (9th Cir. 2004) (assuming that compulsory blood tests for DNA data banking implicate Fourth Amendment interests).

⁵⁵⁹ See sample results from my survey of 30 persons to determine their view on DNA privacy and See *Compare* Question USYANKP.98015Q22A, Roper Center for Public Opinion Research (1998) (reporting that sixty-six percent of respondents answered "yes" to the question, "Do you think the police should or should not be allowed to collect DNA information from suspected criminals—similar to how they take fingerprints?"), with Question USYANKP.98015Q21, Roper Center for Public Opinion Research (1998) (reporting that ninety-five percent of respondents answered "no" to the question, "Do you think employers should or should not be able to obtain access to employees' genetic record, or DNA, without their permission?"), and Question USYANKP.98015Q20, Roper Center for Public Opinion Research (1998) (reporting that ninety-four percent answered "no" to the question, "Do you think insurance companies should or should not be able to obtain access to a person's genetic record, or DNA, without his or her permission?). One distinction that might be drawn in these responses is that respondents change their opinions based upon who asks for the information, i.e., government or private employers. Another inference that might be drawn here, however, is the distinction the public might make between themselves and those they believe have forfeited certain rights to privacy.

⁵⁶⁰ See Kimmelman, "Risking Ethical Insolvency," 216 (drawing comparison between DNA privacy concerns and those related to census). See also Holmes, "Returns of Long Census Forms," A18 (noting "concern among census officials" that privacy worries would lead to refusals to complete census forms); El Nasser, "Census Shaken by Grumbling," A4 (noting widespread privacy concerns regarding 2000 Census fifty-three-question "long form" survey).

no legal justification or barriers to collect abandoned DNA. On a similar vein, even though a population-wide database is yet only a topic of policy debates, there is reason to view this idea with skepticism. Questions about the ethics of forensic DNA testing from databases are currently being raised overseas as well. In the UK, law enforcement can utilize this technology to solve only heinous crimes whereas in Poland, it is restricted to finding victims of war such as missing persons or body identification.⁵⁶¹ However, it would be unwise—and possibly too late—to wait until unintended consequences of technological innovation and mandatory gene banking, albeit developed with well-meaning intentions, are upon us before we consider appropriate responses when the legal means to do so exist now.

Given the considerations discussed above, greater restrictions are recommended than those that exist now on the collection and banking of DNA, whether collected voluntarily or surreptitiously. If courts have been comfortable in rejecting challenges to mass DNA collection because targets are convicts or parolees, surreptitiously taken DNA removes the distinction between offenders and the general public. On deciding upon such a legal challenge, a court may yet find that collecting abandoned DNA is a Fourth Amendment search, and, therefore, requires either a warrant or at least some degree of Fourth Amendment scrutiny. Such an outcome seems unlikely, though, given the current state of Fourth Amendment jurisprudence. If greater protection is to be accorded to abandoned DNA, it is unlikely to arise from Fourth Amendment law.⁵⁶² Instead,

⁵⁶¹ Granja and Machado, “Ethical Controversies of Familial Searching,” 19.

⁵⁶² See Kaye and Smith, “DNA Identification Databases: Legality,” 437 (citing representative cases). (“[U]nder existing doctrine, the Fourth Amendment is quite porous to determined efforts by police to acquire the DNA of specific individuals and of large classes of individuals. . .”). The Court itself has shown some concern about the “power of technology to shrink the realm of guaranteed privacy. . .” See *Kyllo v. United States*, 533 U.S. 27, 33–34 (2001).

governments can offer flexibility and greater protection where judicial interpretation of the Fourth Amendment falls short.⁵⁶³

However, governmental involvement may also present a conflict of interest conundrum as they cross swords with law enforcement who are public officials. This is an obvious disincentive to increasing restrictions on DNA collection. Thus, the most obvious limit might be to require, in the absence of consent, a warrant whenever police seek abandoned DNA from a targeted person.⁵⁶⁴ This burdens the police no more than in cases where they must seek a DNA sample directly from a suspect by means of blood or saliva, but does provide, at a minimum, notice to a suspect that he or she is a target. An even more modest but still desirable regulatory improvement would be for legislatures to clarify the applicability of DNA database laws, both federal and state, to the collection of abandoned DNA.⁵⁶⁵ Because the law has been ambiguous on this point, greater restrictions on the access to and retention of all DNA samples (as opposed to merely their profiles) must be addressed.

Finally, if a legislature decides that a population-wide databank is desirable for criminal justice purposes, we still must pay careful attention to privacy protections. Such protections should not only restrict the access of private insurers and employers to this

⁵⁶³ Indeed, in a thoughtful article about the legal characterizations of body parts and tissue from a British perspective, Jean McHale urges that “the legal regulation of bodily products is a matter which should *not* be left for resolution to *ad hoc* judicial determination....” See McHale, “Waste, Ownership and Bodily Products,” 123, 133 (emphasis added).

⁵⁶⁴ Kerr notes that in the realm of computer crime, Congress now places greater statutory restrictions on police efforts to obtain customer information from Internet service providers than what is called for under the Fourth and Fifth Amendments. See Kerr, “The Fourth Amendment,” *supra* note 13, at 309–10.

⁵⁶⁵ For all kinds of DNA samples, genetic privacy would be further protected by use restrictions that are spelled out before the actual seizure of the sample itself. *Cf.* Krent, *supra* note 25, at 77–93 (arguing for such Fourth Amendment use restrictions even where the initial search and seizure is reasonable).

data but should also restrict the government itself. While DNA evidence has an important role in police investigation, its use in profiling and predictions on criminal behavior should be prohibited until the underlying scientific studies and ethical issues are resolute.

Typically, ethical issues include those related to racial or ethnic group profiling as discussed previously in the case of the Louisiana serial killer and the targeting of the Uighur population in China.⁵⁶⁶ In the future, the possibility of gender profiling may also exist where stereotypical assumptions could adversely impact crime solving. Scientific studies must conclusively and clearly show that there is a single crime gene or a family of genes that are causally related to criminal conduct. Studies to date have pointed to the existence of such a gene but lack appropriate animal models where such candidate genes may be studied in isolation and knock-out mutations of those genes show reversal in protracted antisocial behavior.⁵⁶⁷

Recognizing the need to address these issues, residents of the Australian state of Victoria have called for laws banning “covert DNA sampling” by local police, who admitted to using the same tactics that have been described here to confirm or eliminate suspects in their investigations.⁵⁶⁸ Similarly, there have been calls to action in democratic societies in other parts of the world to examine privacy concerns of citizens. One such

⁵⁶⁶ *Supra* note 333; Wade, “Unusual Use of DNA,” A28; Regalado, “How US experts helped China,” at <https://www.technologyreview.com/f/613000/how-us-experts-helped-china-build-a-dna-surveillance-state/>; Wee, “China uses DNA to track,” at <https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html>.

⁵⁶⁷ Cloninger et al., “Predisposition to Petty Criminality,” 1242-1247; Mednick et al., “Genetic Influence in Criminal Convictions,” 891- 894; Cadoret et al., “Genetic-environmental Interaction in the Genesis,” 916-924; Bruner et al., “Abnormal Behavior Associated with a Point,” 578-580; Delisi et al., “The Etiology of Criminal Onset,” 217-233; Beaver et al., “Evidence of a Gene X Environment Interaction,” 620-645.

⁵⁶⁸ Murphy, “Call for Ban on Covert,” 6. Some police departments outside of Victoria are using the technique as well. See Yamine, “How a Hand-Rolled Cigarette,” 15 (describing police collection of suspect’s cigarette butt that matched sample at murder scene).

voice comes from New Zealand. Increased sophistication of forensic DNA analysis kits combined with the lack of regulation of information extraction from DNA has raised serious concerns about privacy protection. This has prompted a call to action by an independent Law Commission to simplify and overhaul The New Zealand Criminal Investigations Bodily Samples (CIBS) Act of 1995. As a matter of fact, a new Act is being demanded by the Law Commission.⁵⁶⁹

Using the everyday items found in the home, Victoria, Australia, police would obtain DNA from coffee cups, cigarettes, and clothing.⁵⁷⁰ A DNA match found as a result of such sampling would prompt Victoria police to file a formal application to obtain a sample.⁵⁷¹ Police officials conceded that no protocols existed to regulate the collection, storage, or accidental inclusion of these DNA samples into the national DNA databank.⁵⁷² In response to vehement objection by public legal and privacy advocates, Victoria's attorney general has recently promised to examine the "legal loophole" and to review the lack of precautions on the practice.⁵⁷³

In the field of Internet law, commentators have suggested that the label of cyberspace as a "place" has led to disastrous public policy consequences.⁵⁷⁴ Likewise, in

⁵⁶⁹ White et al., "The Use of DNA," 71, 86.

⁵⁷⁰ See Australian Associated Press, "Police Are Secretly Taking."

⁵⁷¹ See Murphy, "Call for Ban on Covert," *supra* note 36.

⁵⁷² See, e.g., Giles, "Secret DNA Tests: Innocent," 3 (noting police concession that no protocols existed for covert DNA collection); Giles, "Tighter DNA Laws," 14 (noting that there are no regulations to prevent samples from "being mistakenly registered on the DNA database for criminals.").

⁵⁷³ See Giles, "Tighter DNA Laws," *supra* note 40.

⁵⁷⁴ See, e.g., Hunter, "Cyberspace as Place," 519 (suggesting that "[w]e may already be past the point where we can do anything about" the cyberspace as place metaphor); Lemley, "Place and Cyberspace," 542 (observing that cyberspace as place metaphor "will serve its purpose only if we understand its limitations.").

the collection of DNA evidence, our labeling and framing of the issue matters. Using the phrase “covert involuntary sampling” eliminates the implied volition that is absent when DNA is collected after it has been shed with a person’s knowledge or consent.

Conclusion

Unregulated collection and banking of DNA by police and profit motivated companies threatens the privacy rights of everyone. Advances in biomedical research, molecular genetics and genealogy are solving cold cases, helping to re-connect families and satiating the curiosity of those who wish to learn about their ethnic heritage. The expected success rate of public demand for genealogy is spawning the growth of private companies that have begun to develop commercial, over the counter self-help genealogy kits.

On the one hand, while these conveniences may be viewed as positive outcomes of research and development, laws must be in place to protect citizens from being exploited for the genetic information that is being given up in exchange for these conveniences on the other hand. When state-operated forensic DNA laboratories were surveyed, the results indicated overwhelming support for not only the procedure but also the manner in which personnel received training and legal assistance, suggesting that reasons for concern are not from unethical conduct by law enforcement officials.⁵⁷⁵ Similarly, privacy concerns with regard to universal DNA databases, which have raised concerns among some, have been downplayed by a Stanford University legal scholar who asserts that such systems can be, in fact, airtight when constructed properly and regulated

⁵⁷⁵ Debus-Sherrill and Field, “Familial DNA Searching,” 20-28.

carefully from their inception. Such efforts would result in greater efficiency, more protection and less invasion in investigative techniques.⁵⁷⁶

Lauded for its forward thinking and timeliness by those interested in genetic privacy, the Genetic Information Nondiscrimination Act (GINA) that became law in 2008 has legal loopholes that need to be filled. GINA does not cover privacy of information with regard to schools, mortgage lending, or housing, and it excludes forms of insurance like life insurance, long-term care, and disability insurance. While genealogy firms welcomed GINA with enthusiasm, scholars view it with skepticism and caution that this is only the first step toward ensuring genetic privacy.

At present, there is no law formulated to guarantee privacy of genetic information, especially because DNA that has been unintentionally discarded due to common everyday occurrences has been likened to trash, allowing anybody—including law enforcement—to obtain it without permission. Consumers of genealogy tests might be unaware of the downstream consequences of giving up their DNA to companies who, in turn, may sell that information to big pharmaceutical firms. Recently, 23andMe, a genealogy firm received a \$300 million investment from a well-known biopharmaceutical company, GlaxoSmithKline, that is dedicated to developing therapeutic drugs for diseases. It is not implausible that GlaxoSmithKline has an interest in obtaining 23andMe's genetic database to further their interest in drug development and sales. Further advances in molecular genetics research could permit ever greater exploitation of that personal information albeit unintentionally. Gain in some spheres results in concomitant loss of personal privacy in other areas. Therefore, the inclusion of DNA as

⁵⁷⁶ Dedrickson, "Universal DNA Databases," 647.

private property within the framework of the Fourth Amendment is worthy of serious consideration and must be put forth to lawmakers. More reasons for DNA protection are discussed below.

First, while Fourth Amendment law may not appear to protect a privacy interest in the human tissue left behind as the debris of our daily lives, it is far from obvious that people do not harbor a privacy expectation in genetic information that society is prepared to recognize as reasonable. While it may be extremely difficult to sympathize with serial killers who are convicted as a result of their shed saliva or blood, few would characterize genetic information as lacking any protection in these circumstances. Many of us may not have faced such a challenge to our privacy yet.

Second, there may be no helpful comparisons between DNA, whether abandoned unknowingly or given up voluntarily, and the way in which body parts and bodies are treated. Given the kind of personal information that may be extracted from even a very small sample containing DNA, there are real limitations to comparing abandoned DNA to fingerprints, body parts, and human waste. As a result, courts and legislatures should consider abandoned DNA as part of a human body, not as a separate category or trash.

Another possible analogy might lie between DNA and the human body or its parts. In assessing the ownership rights over human tissue and cells, the Congressional Office of Technology Assessment once asked whether an analogy between cells and body parts would be fruitful.⁵⁷⁷ Practically speaking, one cannot abandon one's liver or body while alive, but what of corpses and donated or excised organs? Here, the law is not well settled, it seems. Items from the human body like livers, hearts, lungs, and skin "lie in a

⁵⁷⁷ See Office of Technology Assessment, "New Developments in Biotechnology," <https://www.princeton.edu/~ota/disk2/1987/8719/8719.PDF>.

legal limbo.”⁵⁷⁸ Such body parts often have been characterized in terms of quasi-property rights. Body parts may be designated for donation although federal law forbids their outright sale.⁵⁷⁹ Further, courts and legislatures should look within the Fourth Amendment context to expand its definition of private property to include human cellular matter including its genetic material, namely DNA.

Third, even if the collection of DNA were folded into the guidelines used for the banking of DNA from those convicted or arrested, more scrutiny is required regarding how this DNA can be used. There remain many questions about its potential uses (including DNA held in databases) that cannot be easily allayed with the claim that only “junk” DNA is retained for identification purposes. While legislatures have been swift to enact collection statutes, they have been much less clear and responsive to concerns regarding the longer-term handling, storage, and use of samples and records.

It may be that we are already moving toward a system in which the government will have access to the genetic information of everyone in the population,⁵⁸⁰ which will

⁵⁷⁸ Rao, “Property, Privacy and the Human Body,” 359, 375 (2000). On the other hand, the ability to sell human eggs, sperm, blood, teeth, and hair has been widely recognized. See, e.g., Boyd, “Considering a Market in Human Organs,” 417, 461 (2003) (noting accepted categories of marketable bodily products).

⁵⁷⁹ See Rao, “Property, Privacy and the Human Body,” *supra* note 79, at 375.–76. The National Organ Transplant Act makes it a crime to “transfer any human organ for valuable consideration for use in human transplantation if the transfer affects interstate commerce.” See 42 U.S.C. § 274e(a) (2000).

⁵⁸⁰ While most states began their DNA databanks by limiting sample collection to sex offenders, most have since expanded considerably the categories of applicable offenses and persons. For instance, the recent passage of Proposition 69 by California’s voters will permit the collection of DNA, beginning in 2009, from any adult arrested for or charged with a felony. See CAL. PENAL CODE § 296(a)(2) (West 2005). Moreover, Fourth Amendment analysis presents no obvious bar to the use of the nearly 300 million DNA samples sitting in tissue repositories. See Kaye and Smith, “DNA Identification Databases,” *supra* note 12, at 436–37. Future developments will only make DNA-based identification easier. Australian scientists already have patented a document that stores DNA in a sealed packet: one step towards the concept of using DNA swipes instead of signatures to verify one’s identity. See Cauchi, “Saliva, Blood and Skin,” A3.

be used to solve crimes ranging from murders to littering.⁵⁸¹ If we want unrestricted government access to DNA information, however, that ought to be the subject of public debate rather than made possible through means such as analogizing DNA to trash by law enforcement or through moral hazard post collection by private companies.

The real objections here are not to the use of DNA data banking itself. As social theorist David Garland observes, surveillance technologies are an essential part of modern societies that require some means of data gathering.⁵⁸² One day DNA identification for the entire population may indeed be as ordinary as the Social Security number, or as mundane as a t-shirt slogan.⁵⁸³ The problem that is raised acutely is that the means by which total population DNA data banking might be achieved have arrived without general public awareness and thus without discussion of how it may be regulated against abuse. Without meaningful consideration of genetic privacy and how our DNA is treated, we collectively stand to lose the ability to protect our genetic information.

⁵⁸¹ DNA testing for minor crimes has already begun. In the British county of Yorkshire, South Yorkshire police have issued bus drivers DNA swab kits so that passengers who spit on them may be prosecuted successfully. See Dunlop, "Bus Drivers Get DNA," 8.

⁵⁸² See Garland, "Panopticon Days: Surveillance and Society," 3.

⁵⁸³ One company offers the opportunity to have your DNA analyzed and to print its "snapshot" on t-shirts and mugs. See Holleman, "Want Your DNA Encoded," E1.

Appendix 1.

Survey Results

P.C.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	Yes? I have already tested with ancestry.com. I am not aware of long lost relatives, but a few distant relatives have reached out. One surprise was a distant cousin who lives in Italy.
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	Yes, I would like to know more details about my ancestry; as the tests become better, they have more specificity.
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	Yes, I've already had mine tested with ancestry.com and would like to try 23 and me. Not familiar with heritage.com
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	YES, I do have concerns. . .I didn't think much about it when I sent in my sample.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	YEs, I do have concerns with government genetic databanks as well.
Question 6: How many generations has your family lived in the USA?	I am the 3rd generation.
Question 7: Are you aware of DNA fingerprinting?	I have a vague idea, our DNA might be used just like a finger print?

A. K. G.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	Not particularly
--	------------------

Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	Ancestry
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	Maybe
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	I'm not sure
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	Concerns about privacy
Question 6: How many generations has your family lived in the USA?	0
Question 7: Are you aware of DNA fingerprinting?	Yes

J. R. R.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	No.
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	I wouldn't do DNA testing along the lines described here, so N/A.
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com,myheritage.com?	No (or N/A)
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	Plenty concerned. And unlike many other facets of my "privacy," this one would potentially affect my kids too.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	No, it would not be safe beyond doubt in a government databank.
Question 6: How many generations has your family lived in the USA?	Three or four generations in the case of three of my four grandparents (the Jewish ones). In one case (the Scots-Irish family of my paternal grandmother), much longer - possibly back to the 18th century.
Question 7: Are you aware of DNA fingerprinting?	Yes, though I don't have a strong technical / scientific understanding of it.

H. F.

Question 1: Would you be interested in determining your ancestry or finding long lost	I am interested in ancestry.
---	------------------------------

relatives?	
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	Primarily ancestry. However, I would be interested in finding my grandfather on my father's side. But I'm not interested in finding anymore relatives beyond that.
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	No, never.
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	I have major concerns about privacy and do not trust any of those companies.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	I would never want my DNA stored in a governmental databank. I feel that the government would eventually come up with a reason to justify using the DNA in a way that could be detrimental to the poor and powerless.
In the same way the justice system is rigged for the rich and powerful, a governmental databank could be treacherous for certain populations.	People who are disadvantaged have very little recourse in a system that is stacked against them and are therefore vulnerable. I believe it would be dangerous for them and others to have their DNA stored in a governmental databank.
Question 6: How many generations has your family lived in the USA?	My mother is Cape Verdean, mixed european, african race. Her parents were born in the Cape Verde Islands, owned by Portugal at the time and spoke Portuguese. My mother is second generation. My father's family includes Native American ancestry, Cherokee, and others are descendants of slaves. So some of his ancestors were the original Americans.
Question 7: Are you aware of DNA fingerprinting?	No, I have never heard of it.

J.B.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	yes
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	Both
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	Not sure
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	Yes, I do have some concerns. I would wonder if insurance companies would use the info to determine any Pre-

	existing conditions.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	Yes, concerns for the same reason as listed above.
Question 6: How many generations has your family lived in the USA?	I am not sure, several generations
Question 7: Are you aware of DNA fingerprinting?	yes.

E.D.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	No
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	No
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	No
Question 4: Do you have any concerns about privacy	Yes
OR do you feel that your DNA will be safe in the hands of private companies?	No
Question 5: Do you have any concerns about privacy	Yes
OR do you feel that your DNA will be safe in the hands of a government genetic databank?	No
Question 6: How many generations has your family lived in the USA?	Lots
Question 7: Are you aware of DNA fingerprinting?	Yes

L.S.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	Yes
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	Both
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	No
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	No, I do not believe the information is safe. Recently there were 2 criminal cases where DNA from the Ancestry.com was matched

	through family information. To me, that means my information is also not private. I don't want anyone knowing that much about me.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	No, see question 4 response
Question 6: How many generations has your family lived in the USA?	2
Question 7: Are you aware of DNA fingerprinting?	Yes, same response as 4.

S. S.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	yes
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	ancestry
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com, myheritage.com?	I already did this
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	safe
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	safe
Question 6: How many generations has your family lived in the USA?	Don't know
Question 7: Are you aware of DNA fingerprinting?	Yes

S.H.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	Possibly, yes—if that is a fair response. Maybe
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH	I am curious about my ancestry, but I am not sure that I would put a lot of my own time into finding a lot about it.
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com,myheritage.com?	I would not be willing to send my DNA to anyone

Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	I do have concerns. I feel that these companies could benefit greatly from the information that they receive from people, much more than those that give their DNA can benefit. One is giving a company vast amounts of personal information with DNA, with no clear idea what will happen to it, and what kind of information, is on then file somewhere, and could possibly be used for research, or revealed to someone else, without your consent.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	I would not want my DNA in a government genetic databank
Question 6: How many generations has your family lived in the USA?	Paternal side: 2 generations (my father was born in Russia, so I count two, but maybe I am not counting correctly) Maternal side: 3 my mother was born in the USA, bother her parents arrived here as young adults.
Question 7: Are you aware of DNA fingerprinting?	Yes, but I don't know enough about it to really understand it completely or coherently explain it to anyone myself.

V. H.

Question 1: Would you be interested in determining your ancestry or finding long lost relatives?	Sure
Question 2: Would it be to determine ancestry, finding long lost relatives or BOTH?	Both
Question 3: if yes, would you be willing to send your DNA to a private gene bank like 23 and Me, Ancestry.com,myheritage.com?	Yes I have already participated in Ancestry.com.
Question 4: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of private companies?	I feel safe with Ancestry.com.
Question 5: Do you have any concerns about privacy OR do you feel that your DNA will be safe in the hands of a government genetic databank?	I feel safe.
Question 6: How many generations has your family lived in the USA?	3
Question 7: Are you aware of DNA fingerprinting?	No

References

- 23andMe, Inc. 2019. <https://www.23andme.com/>.
- Agarwal, Prateek. "Asymmetric Information." *Intelligent Economist*, April 10, 2019. <https://www.intelligenteconomist.com/asymmetric-information/>.
- Alfano, Justin A. "Look What Katz Leaves Out: Why DNA Collection Challenges the Scope of the Fourth Amendment." *Hofstra Law Review* 58, no. 4 (2005): 1017-1047.
- Allen, Anita L. "Genetic Privacy: Emerging Concepts and Values." In *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, edited by Mark A. Rothstein, 47-100. Washington, DC: USDOE Office of Energy Research, 1998.
- Allison, M. "Industry Welcomes Genetic Information Nondiscrimination Act." *Nature Biotechnology* 26, no. 6 (2008): 596-597. doi:10.1038/nbt0608-596c.
- Allison, Malorye. "Is Personalized Medicine Finally Arriving?" *Nature Biotechnology*, (2008): 509-517. doi:10.1038/nbt0508-509.
- Allison, Malorye. "Trouble at the Office." *Nature Biotechnology* 26 (2008): 96-99.
- Alschuler, Albert W. "Regarding Re's Revisionism: Notes on 'The Due Process Exclusionary Rule'." *Harvard Law Review* 127, no. 8 (2014): 302-324.
- Amsterdam, Anthony G. "Perspectives on the Fourth Amendment." *Minnesota Law Review* 58 (1973): 349.
- Andrews, Lori B. "Predicting and Punishing Antisocial Acts: How the Criminal Justice System Might Use Behavioral Genetics." In *Behavioral Genetics: The Clash of Culture and Biology*, edited by Ronald A Carson and Mark A. Rothstein, 116-155. Baltimore, MD: Johns Hopkins University Press, 1999.
- Annas, George J. "Genetic Privacy: There Ought to Be a Law." *Texas Review of Law & Politics* 4, no. 1 (1999): 9.
- Annas, George J., Leonard H. Glantz, and Patricia A. Roche. *The Genetic Privacy Act and Commentary*. Washington, DC: Human Genome Project, 1995.

- Apse, Kira A., Barbara B. Biesecker, Francis M. Giardiello, Barbara P. Fuller, and Barbara A. Bernhardt. "Perceptions of Genetic Discrimination among At-Risk Relatives of Colorectal Cancer Patients." *Genetics in Medicine* 6 (2004): 510-516. doi:10.109701.GIM.0000144013.96456.6C.
- Australian Associated Press. "Police Are Secretly Taking DNA Samples." *AAP News*, November 22, 2004.
- Axelrad, Seth. "Survey of State DNA Database Statutes." *American Society of Law, Medicine, & Ethics* (2005). http://www.aslme.org/dna_04/grid/guide.pdf.
- Bachner-Melman, Rachel, Christian Dina, Ada H. Zohar, Naama Constantini, Elad Lerer, Sarah Hoch, Sarah Sella, et al. "AVPR1a and SLC6A4 Gene Polymorphisms Are Associated with Creative Dance Performance." *PLOS Genetics* 1, no. 3 (2005): e42. doi:10.1371/journal.pgen.0010042.
- Ballantyne, Kaye N., Victoria Keerl, Andreas Wollstein, Ying Choi, Sofia B Zuniga, Arwin Ralf, Mark Vermeulen, Peter de Kniff, and Manfred Kayser. "A New Future of Forensic Y-chromosome Analysis: Rapidly Mutating Y-STRs for Differentiating Male Relatives and Paternal Lineages." *Forensic Science International: Genetics* 6, no. 2 (2012): 208-218. doi:10.1016/j.fsigen.2011.04.017.
- BBC News*. "Brick Thrower Jailed over Death." April 19, 2004.
- BBC News*. "Killer Caught by Relative's DNA." April 19, 2004.
- Beaver, Kevin M., John Paul Wright, Matt Delisi, Leah E. Daigle, Marc L. Swatt, and Chris L. Gibson. "Evidence of a Gene X Environment Interaction." *International Journal of Offender Therapy and Comparative Criminology* 51, no. 6 (2007): 620-645.
- Bieber, Frederick R. "Science and Technology of Forensic DNA Profiling: Current Use and Future Predictions." In *DNA and the Criminal Justice System: The Technology of Justice*, edited by David Lazer, 23-62. Cambridge, MA: Massachusetts Institute of Technology, 2005.
- Bieber, Frederick R., Charles H. Brenner, and David Lazer. "Finding Criminals through DNA of Their Relatives." *Science*, June 2, 2006: 1315-1316. doi:10.1126/science.1122655.
- Boyd, S. Gregory. "Considering a Market in Human Organs." *North Carolina Journal of Law & Technology* 4, no. 2 (2003): 417-461.

- Brown, DeNeen L. "Can the 'Immortal Cells' of Henrietta Lacks Sue for Their Own Rights?" *Washington Post*. June 25, 2018.
- Brunner, H. G., M. Nelen, X. O. Breakefield, and B. A. van Oost. "Abnormal Behavior Associated with a Point Mutation in the Structural Gene for Monoamine Oxidase A." *Science* 262, no. 5133 (1993): 578-580.
- Brunner, Jordan, and Emma Kohse. "Supreme Court Grants Cert in *Carpenter v. United States*: An Overview." *Lawfare*, June 6, 2017.
- Budowle, Bruce, F. Samuel Baechtel, Catherine T. Comey, Alan M. Giusti, and Leonard Klevan. "Simple Protocols for Typing Forensic Biological Evidence: Chemiluminescent Detection for Human DNA Quantitation and Restriction Fragment Length Polymorphism (RELP) Analyses and Manual Typing of Polymerase Chain reaction (PCR) Amplified Polymorphisms." *Electrophoresis* 16, no. 9 (1995): 1559-1567. doi:10.1002/elps.11501601259.
- Budowle, Bruce, Tamyra R Moretti, Stephen J. Niezgod, and Barry L. Brown. "CODIS and PCR-based Short Tandem Repeat Loci: Law Enforcement Tools." *Proceedings of the Second European Symposium on Human Identification*. Madison, WI: Promega Corporation, 1998.
- Bunkley, Nick. "Dutch Carmaker Still Pushing to Buy Saab." *New York Times*, January 12, 2010.
- Butler, John M. *Forensic DNA Typing: Biology, Technology, and Genetics of STR Markers*. 2nd ed. Boston: Elsevier Academic Press, 2005.
- Cadoret, R. J., W. R. Yates, E. Troughton, G. Woodworth, and M. A. Stewart. "Genetic-environmental Interaction in the Genesis of Aggressivity and Conduct Disorders." *Archives of General Psychiatry* 52, no. 11 (1994): 916-924.
- Caramanica, Jon. "Dapper, Privileged and Unapologetic." *New York Times*, January 16, 2010.
- Cauchi, Stephen. "Saliva, Blood and Skin to Seal Deal for Kith and Kin." *The Age*, June 1, 2004.
- Cheon-Hayes, Aileen. "Stillman to Grant: When Form Becomes Substance." Paper presented at the National Criminal Justice Conference: Seven, Eight, Night: Silence, Searches and Detention, Vancouver, BC, April 2012.

- Cloninger, C. Robert, Soren Sigvardsson, and Michael Bohman. "Predisposition to Petty Criminality in Swedish Adoptees." *Archives of General Psychiatry* 39, no. 11 (1982): 1242-1247. doi:10.1001/archpsych.1982.0429011001002.
- Cloud, Morgan. "Rube Goldberg Meets the Constitution." *Mississippi Law Journal* 72 (2002): 5-50.
- Colb, Sherry F. "Is Your Scalp a Constitution-Free Zone? A Federal Appeals Court Approves Suspicionless Hair Sampling." *FindLaw*. November 17, 2004.
- Cole, Simon A. "Is the 'Junk' Designation Bunk?" *Northwestern Law Review*, September 4, 2007.
- . *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA: President and Fellows of Harvard College, 2001.
- Collins, Francis S. *The Language of Life: DNA and the Revolution in Personalized Medicine*. New York: Harper, 2010.
- Council of the European Union. "Treaty Prum." 2005.
<http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf>.
- Curley, Robert A., and Lisa M. Caperna. "The Brave New World is Here: Privacy Issues and The Human Genome Project." *Defense Counsel Journal* 70, no. 1 (2003): 22-35.
- Davies, Kevin. *Cracking the Genome: Inside the Race to Unlock Human DNA*. New York: Free Press, 2001.
- Debus-Sherrill, Sara, and Michael B Field. "Familial DNA Searching: An Emerging Forensic Investigative Tool." *Science & Justice* 59, no. 1 (2019): 20-8.
- deCODE Genetics. n.d. <https://www.decode.com/>.
- Dedrickson, Kirsten. "Universal DNA Database: A Way to Improve Privacy?" *Journal of Law and Biosciences* 647 (2018). doi:10.1093/jlb/lxx041.
- Delisi, Matt, Kevin M. Beaver, John Paul Wright, and Michael G Vaughn. "The Etiology of Criminal Onset: The Enduring Salience of Nature and Nurture." *Journal of Criminal Justice* 36, no. 3 (2008): 217-33. doi:10.1016/j.crimjus.2008.04.001.
- Dispatch Staff. "Convicted Murderer Donald Sigsbee Dies in Prison." *Oneida Daily Dispatch*, October 28, 2009.

- Dodd, Mike. "Why Can't Cubs Win?" n.d. <http://www.usatoday.com>.
- Ducharme, Jamie. "A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?" *Time Magazine*, July 26, 2018.
- Dunlop, Emma. "Bus Drivers Get DNA Swab Kits to Catch Assailants Who Spit." *Yorkshire Post*, January 21, 2005.
- Duster, Troy. *Backdoor to Eugenics*. 2nd ed. New York: Routledge, 2003.
- . "Race and Reification in Science." *Science* 307, no. 5712 (February 18, 2005): 1050-1051.
- Dyck, Rand. *Canadian Politics: Critical Approaches*. 3rd ed. Scarborough, ON, CAN: Nelson Thomson Learning, 2000.
- . *Canadian Politics: Critical Approaches*. Concise Ed. Toronto, ON: Nelson Education, 1992.
- Edwards, A., A. Civitello, H. A. Hammond, and C. T. Caskey. "DNA Typing and Genetic Mapping with Trimeric and Tetrameric Tandem Repeats." *American Journal of Human Genetics* 49, no. 4 (1991): 746-56.
- El Nasser, Haya. "Census Shaken by Grumbling." *USA Today*, April 10, 2000.
- Ellement, John R. "20 Years after His Murder, Prosecutor is Remembered." *Boston Globe*, September 25, 2015.
- Epstein, Jules. "'Genetic Surveillance': The Bogyman Response to Familial DNA Investigations." *Journal of Law, Technology and Policy* 1 (2009): 141.
- Farias, Cristian. "He Won a Landmark Case for Privacy Rights: He's Going to Prison Anyway." *New York Times*, June 13, 2019.
- Farmer, Brit M. "Using Genetic Genealogy to Convict Raymond Charles Rowe." *60 Minutes: Overtime*, January 9, 2019.
- FEDAgent. "On Remand from the Supreme Court, the Sixth Circuit Applies the Good Faith Exception in Carpenter." June 13, 2019.
- Federal Bureau of Investigation. *NDIS Participants*. 2005. <http://www.fbi.gov/hq/lab/codis/partstates.htm>.

- . *Quality Assurance Standards for Forensic DNA Testing Laboratories*. 2011. <http://www.fbi.gov/file-repository/quality-assurance-standards-for-forensic-dna-testing-laboratories.pdf/view>.
- . *The FBI's Combined DNA Index System Program*. 2000. <http://www.fbi.gov/hq/lab/codis/brochure.pdf>.
- Forensic Genetics Policy Initiative. *Establishing Best Practice for Forensic DNA Databases*. 2017. <http://dnapolicyinitiative.org/wp-content/uploads/2017/08/BestPractice-Report-plus-cover-final.pdf>.
- Francescani, Christopher. "Sex Fiend Admits He Killed 5 in Brooklyn." *New York Post*, March 10, 2001.
- Frudakis, Tony N. *Molecular Photofitting: Predicting Ancestry and Phenotype Using DNA*. Burlington, MA: Academic Press, 2008.
- Garland, David. "Panopticon Days: Surveillance and Society." *Criminal Justice Matters* 3, no. 1 (1995): 3-4.
- Gartrell, Nate. "Retired Cold Case Investigator Tracked the 'Golden Gate Killer' to His Door." *Mercury News*, April 26, 2018.
- Geggel, Laura. "23andMe Is Sharing Its 5 Million Clients' Genetic Data with Drug Giant GlaxoSmithKline." *Live Science*, July 26, 2018.
- Genetics and Public Policy Center. *U.S. Public Opinion on Uses of Genetic Information and Genetic Discrimination*. Washington, DC: Pew Charitable Trusts, 2007.
- Genetics Generation. *Genetic Information Nondiscrimination Act of 2008 (GINA)*. 2015. <http://knowgenetics.org/genetic-information-nondiscrimination-act-of-2008-gina/>.
- GenomeWeb. *Life Technology Acquires Consumer Genetics Testing Firm Navigenics*. July 17, 2012. <https://www.genomeweb.com/diagnostics/life-technologies-acquires-consumer-genetics-testing-firm-navigenics#.XQZacrXhPy>.
- Giles, Tanya. "Secret DNA Tests: Innocent People's Samples Collected." *Herald-Sun*, November 22, 2004.
- . "Tighter DNA Laws." *Herald-Sun*, November 23, 2004.

- Gill, P., L. Fereday, N. Morling, and P. M. Schneider. "The Evolution of DNA Databases: Recommendations for New European STR Loci." *Forensic Science International* 156, nos. 2-3 (2006): 242-244.
- Gillespie, Elizabeth M. "Need for Greed Ends with 'Cold Case' Arrest." *Los Angeles Times*, June 1, 2003.
- GlaxoSmithKline. *GSK and 23andMe Sign Agreement to Leverage Genetic Insights for the Development of Novel Medicines*. July 25, 2018. <https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines/>.
- Gordon, Tony. "DNA Sample Links Man to Burglary." *Chicago Daily Herald*, July 3, 2001.
- Gosch, Elizabeth. "Great-Grandmother's Killer Caught by Cigarette DNA." *Australian*, February 16, 2005.
- Grand, Jeffrey S. "The Bleeding of America: Privacy and the DNA Dragnet." *Cardozo Law Review* 23, no. 6 (2001): 2277-2323.
- Greally, John M. "Encyclopaedia of Humble DNA." *Nature* 447 (2007): 782-783.
- Greenhouse, Steven. "Law Seeks to Ban Misuse of Genetic Testing." *New York Times*, November 15, 2009.
- Guardian* Staff. "DJ Pleads Guilty to 1992 Murder after Relative's SNA Test Links Him to a Crime." *The Guardian*, January 8, 2019.
- Guterman, Lila. "Scientists Reveal Map of Human Genetic Variation and Warn That It Does Not Reflect Racial Differences." *Chronicle of Higher Education*. April 2005.
- Haag, Matthew. "FamilyTreeDNA Admits to Sharing Genetic Data with F.B.I." *New York Times*, February 4, 2019.
- Halbfinger, David M., and Allison Hope Weiner. "Celebrity Lawyer in Talks about Wiretapping Evidence." *New York Times*, February 25, 2006.
- Hanson, Erin K., and Jack Ballantyne. "A Highly Discriminating 21 Locus Y-STR 'Megaplex' System Designed to Augment the Minimal Haplotype Loci for Forensic Casework." *Journal of Forensic Sciences* 49, no. 1 (2004): 40-51.

- Hare, Breanna, and Christo Taoushiani. "What We Know about the Golden State Killer Case, One Year after a Suspect Was Arrested." *CNN*, April 24, 2019.
- Harmon, Amy. "Lawyers Fight DNA Samples Gained on the Sly." *New York Times*, April 3, 2008.
- . 2007. "Stalking Strangers' DNA to Fill in the Family Tree." *New York Times*, April 2, 2008.
- Hawkes, Jeff, and Tom Knapp. "Raymond 'DJ Freez' Rowe Arrested for 1992 Killing of Schoolteacher Christy Mirack." *Lancaster Online*, June 25, 2018.
https://lancasteronline.com/news/local/raymond-dj-freez-rowe-arrested-for-killing-of-schoolteacher-christy/article_f05a2ee4-78b211e8-ad10-4382ef4296d.html.
- Hazel, J. W., E. W. Clayton, B. A. Lamin, and C. Slobogin. "Is It Time for a Universal Genetic Forensic Database?" *Science* 362, no. 6417 (2018): 898-900.
 doi:10.1126/science.aav5474.
- Herber, Birgit, and Kurt Herold. "DNA Typing of Human Dandruff." *Journal of Forensic Sciences* 43, no. 3 (1998): 648-656. doi:10.1520/JFS16197J.
- Herbert, Alan, Norman P. Gerry, Matthew B McQueen, Iris M. Heid, Arne Pfeufer, Thomas Illig, H.-Erich Wichmann, et al. "A Common Genetic Variant Is Associated with Adult and Childhood Obesity." *Science* 312, no. 5771 (2006): 279-283.
- Herper, Matthew. "23andMe Gets \$300 Million Boost from GlaxoSmithKline to Develop New Drugs." *Forbes*, July 25, 2018.
- Hibbert, Michelle. "DNA Databanks: Law Enforcement's Greatest Surveillance Tool?" *Wake Forest Law Review* 34 (1999): 767-796.
- Higuchi, Russell, Cecilia H. von Beroldingen, George F. Sensabaugh, and Henry A. Erlich. "DNA Typing from Single Hairs." *Nature: International Journal of Science* no. 332 (1988): 543-546.
- Ho, Vanessa. "Man is Sentenced in '82 Killing DNA Solved." *Seattle Post-Intelligencer*, March 6, 2004.
- Hochmeister, Manfred N., Richard Dirnhofer, U. V. Borer, Bruce Budowle, Jong Min Jung, and Catherine T. Comey. "PCR-Based Typing of DNA Extracted from

Cigarette Butts.” *International Journal of Legal Medicine* 104, no. 4 (1991): 229-233. doi:10.1007/BF01369812.

Hochmeister, Manfred. “PCR Analysis of DNA from Fresh and Decomposed Bodies and Skeletal Remains in Medicolegal Death Investigations.” In *Forensic DNA Profiling Protocols*, edited by Patrick J. Lincoln and Jim Thomson, 19-26. Totawa, NJ: Humana Press, 1998.

Hogg, Peter W. *Constitutional Law of Canada*. 5th ed. Toronto, ON: Thompson Reuters Canada, 2019.

Holden, Stephen. “Three Loners on a Road Leading to One Another.” *New York Times*, February 26, 2010.

Holleman, Joe. “Want Your DNA Encoded on a Starbucks Mug?” *St. Louis Post Dispatch*, March 16, 2004.

Holmes, Steven A. “Returns of Long Census Forms Lag: Bureau Cites Privacy Fears.” *New York Times*, April 15, 2000.

Home Office, Forensic Science and Pathology Unit. *DNA Expansion Programme, 2000-2005: Reporting Achievement*. 2005. <http://www.statewatch.org/news/2006/jan/uk-DNA-database.pdf>.

Hopwood, Andy, Armando Mannucci, and Kevin Sullivan. “DNA Typing from Human Faeces.” *International Journal of Legal Medicine* 108, no. 5 (1996): 237-243. doi:10.1007/BF01369817.

Howland, Dave. “Inmate Charged in Prosecutor’s 1995 Murder.” *SouthCoastToday*, February 20, 1998.

Human Rights Watch. *Kuwait: New Counterterrorism Law Sets Mandatory DNA Testing: Violates Right to Personal Privacy*. 2015. <https://www.hrw.org/news/2015/07/20/kuwait-new-counterterrorism-law-sets-mandatory-dna-testing/>.

Hunter, Dan. “Cyberspace as Place and the Tragedy of the Digital Anticommons.” *California Law Review* 91 (2003): 439-519.

Imwinkelried, Edward J., and David H. Kaye. “DNA Typing: Emerging or Neglected Issues.” *Washington Law Review* 76, no. 2 (2001): 413-455.

Innocence Project. 2019. <https://www.innocenceproject.org/>.

- Jeffreys, Alec J. "Genetic Fingerprinting." *Nature Medicine* 11 (2005): 1035-30. doi:10.1038/nm1005-1035.
- Jehl, Laura E., and Jonathan E. Meyer. "Supreme Court Reenters Fray on Privacy: *Carpenter v. United States*." *National Law Review*, June 9, 2017.
- Jobling, Mark A., Matthew Hurles, and Chris Tyler-Smith. *Human Evolutionary Genetics*. New York: Garland Science, 2003.
- Joh, Elizabeth E. "Reclaiming 'Abandoned' DNA: The Fourth Amendment and Genetic Privacy." *Northwestern University Law Review* 100, no. 2 (2006): 857-884.
- Johns Hopkins Medicine. *The Legacy of Henrietta Lacks*. n.d. <https://www.hopkinsmedicine.org/henrietalacks/index.html>.
- Johnson, Tracy. "N.J. Man Convicted of 1982 Murder." *Seattle Post-Intelligencer*, January 22, 2004.
- Joly, Yann, Giacinto Marrocco, and Charles Dupras. "Risks of Compulsory Genetic Databases." *Science* 363, no. 6430 (2019): 938-940. doi:10.1126/science.aaw4347.
- Kaplan, Gisela, and Lesley J. Rogers. *Gene Worship: Moving Beyond the Nature/Nurture Debate Over Genes, Brain, and Gender*. New York: Free Press, 2010.
- Kass, Nancy E. "The Implications of Genetic Testing for Health and Life Insurance." In *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, edited by Mark A. Rothstein, 312-13. New Haven, CT: Yale University Press, 1999.
- Kaye, David H. "Please, Let's Bury the Junk: The CODIS Loci and the Revelation of Private Information." *Northwestern University Law Review Colloquy* 102 (2007): 70-81.
- Kaye, David H. "Science Fiction and Shed DNA." *Northwestern University Law Review: Colloquy* 101 (2006): 62-68. doi:10.2139/ssrn.950572.
- Kaye, David H. "The Science of DNA Identification: From the Laboratory to the Courtroom (and Beyond)." *Minnesota Journal of Law Science & Technology* 8, no. 2 (2007): 409-427.
- Kaye, David H, and Michael E. Smith. "DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage." *Wisconsin Law Review* (2003): 413-459.

- Kerr, Orin S. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution." *Michigan Law Review* 102, no. 5 (2004): 801-888.
- Kevles, Daniel J. *In the Name of Eugenics: Genetics and the Uses of Human Heredity*. New York, 1985.
- Kevles, Daniel J., and Leroy Hood. *The Code of Codes: Scientific and Social Issues in the Human Genome Project*. Cambridge, MA: Harvard University Press, 1993.
- Kimmelman, Jonathan. "Risking Ethical Insolvency: A Survey of Trends in Criminal DNA Databanking." *Journal of Law, Medicine & Ethics* 28 (2000): 209.
- Kolata, Gina. "Bits of Mystery DNA, Far from 'Junk,' Play Crucial Role." *New York Times*, September 5, 2012.
- Korstanje, Ron, and Beverly Paigen. "From QTL to Gene: The Harvest Begins." *Nature Genetics* 31 (2002): 235-236. doi:10.1038/ng0702-235.
- Ku, Raymond S. "The Founders' Privacy: The Fourth Amendment and The Power of Technological Surveillance." *Minnesota Law Review* 86 (2002): 1325-1362.
- LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*. 5th ed. Eagan, MN: Thomson West, 2012.
- "Law 5/2008 Approves the Creation of a DNA Profiles Database for Civil and Criminal Identification Purposes." *Diario de Republica* 1, no. 30 (2008): 962-8.
- Lee, Henry C., Robert E. Gaensslen, Paul D. Bigbee, and J. J. Kearney. "Guidelines for the Collection and Preservation of DNA Evidence." *Journal of Forensic Identification* 41, no. 5 (1991): 344-356.
- Lehrman, Sally. "Prisoners' DNA Database Ruled Unlawful." *Nature* 394 (1998): 818.
- Lemley, Mark. "Place and Cyberspace." *California Law Review* 91 (2003): 521-42.
- Lin, Chin-Hsing, Stacey Hansen, Zhenshan Wang, Daniel R. Storm, Stephen J. Tapscott, and James M. Olson. "The Dosage of the NeuroD2 Transcription Factor Regulates Amygdala Development and Emotional Learning." *Proceedings of the National Academy of Sciences of the United States of America* 102, no. 41 (2005): 14877-14882. doi:10.1073/pnas.0506785102.
- Liptak, Adam. "In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy." *New York Times*, June 22, 2018.

- . “Justices Allow Police to Take DNA Samples after Arrests.” *Wichita Eagle*, June 4, 2013.
- Machado, Helena, and Susana Silva. “‘Would You Accept Having Your DNA Profile Inserted in the National Forensic DNA Database? Why’: Results of a Questionnaire Applied in Portugal.” *Forensic Science International* 8, no. 1 (2014): 132-6. doi:10.1016/j.fsigen.2013.08.014.
- Machado, Helena, and Susanna Silva. “Portuguese Forensic DNA Database: Political Enthusiasm, Public Trust, and Probably Issues in Future Practice.” In *Genetic Suspects: Global Governance of Forensic DNA Profiling and Databasing*, edited by Richard Hindmarsh and Barbara Prainsack, 218-239. Cambridge: Cambridge University Press, 2010.
- Madden, Mary, and Lee Rainie. “Americans’ Attitudes about Privacy, Security and Surveillance.” *Pew Research Center*, May 20, 2015. <https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.
- Maguire, Christopher N., L. A. McCallum, C. Storey, and Jonathan P. Whitaker. “Familial Searching: A Specialist Forensic DNA Profiling Service Utilising the National DNA Database® to Identify Unknown Offenders via Their Relatives—The UK Experience.” *Forensics Science International: Genetics* 8, no. 1 (2014): 1-9. doi:10.1016/j.fsigen.2013.07.004.
- Malayandi, Viba, C. Lerman, N. L. Benowitz, C. Jepson, F. Patterson, and R. F. Tyndale. “Impact of CPY2A6 Genotype on Pretreatment Smoking Behaviour and Nicotine Levels from and Usage of Nicotine Replacement Therapy.” *Molecular Psychiatry* 11, no. 4 (2006): 400-409. doi:10.1038/sj.mp.4001794.
- Martin, Peter D., Hermann Schmitter, and Peter M. Schneider. “A Brief History of the Formation of DNA Databases in Forensic Science within Europe.” *Forensic Science International* 119, no. 2 (2001): 225-231.
- Martinez, F. D. “Genes, Environments, Development and Asthma: A Reappraisal.” *European Respiratory Journal* 29 (2007): 179-184. doi:10.1183/09031936.00087906.
- Mascolo, Edward G. “The Role of Abandonment in the Law of Search and Seizure: An Application of Misdirected Emphasis.” *Buffalo Law Review* 20 (1971): 399.
- Matejik, Laura A. “DNA Sampling: Privacy and Police Investigation in a Suspect Society.” *Arkansas Law Review* 61 (2009): 53-81.

- McHale, Jean. "Waste, Ownership, and Bodily Products." *Health Care Analysis* 8 (2000): 123-133.
- McLellan, Dennis. "John Moore, 56; Sued to Share Profits from His Cells." *Los Angeles Times*, October 13, 2001.
- Mednick, S A., W. F. Gabrielli, and B. Hutchings. "Genetic Influence in Criminal Convictions: Evidence from an Adoption Court." *Science* 225, no. 4651 (1984): 891-894.
- Meyer-Lindenberg, Andreas, Joshua W. Buckholtz, Bhaskar Kolachana, Ahmad R. Hariri, Lukas Pezawas, Giuseppe Blasi, Ashley Wabnitz, et al. "Neural Mechanisms of Genetic Risk for Impulsivity and Violence in Humans." *Proceedings of the National Academy of Sciences of the United States of America* 103, no. 16 (2006): 6269-6274. doi:10.1073/pnas.0511311103.
- Molteni, Megan. "The Future of Crime Fighting Is Family Tree Forensics." *Wired*, December 26, 2018.
- Muenster, John R. "DNA-case Ruses Damage Integrity of Legal System." *Seattle Times*, February 3, 2004.
- Mukherjee, Siddhartha. *The Emperor of All Maladies: A Biography of Cancer*. New York: Scribner, 2010.
- Murphy, Patrick. "Call for Ban on Covert DNA Sampling." *Australian*, November 23 (2004): 6.
- Nakashima, Ellen. "From DNA of Family, a Tool to Make Arrests: Privacy Advocates Say the Emerging Practice Turns Relatives into Genetic Informants." *Washington Post*, April 21, 2008.
- National Cancer Institute. *BRCA Mutations: Cancer Risk and Genetic Testing*. January 30, 2018. <https://www.cancer.gov/about-cancer/causes-prevention/genetics/brca-fact-sheet>.
- National Commission on the Future of DNA Evidence. *What Every Law Enforcement Officer Should Know about DNA Evidence*. Government Report, Washington, DC: National Institute of Justice, 1999.
- National Conference of State Legislatures. *Genetic Privacy Laws*. n.d. <http://www.ncsl.org/issues-research/health/genetic-privacy-laws.aspx>.

- National Policing Improvement Agency. "NDNAD Statistics." n.d. <http://www.npia.police.uk/en/13338.htm>.
- National Public Radio. *All Things Considered: Drafting a Genetic Map of Human Diversity*. 2005. <http://www.npr.org/templates/story/story.php?storyId=4503527>.
- National Research Council Committee on DNA Forensic Science. *The Evaluation of Forensic DNA Evidence*. Washington, DC: National Academies Press, 1996.
- National Research Council. *DNA Technology in Forensic Science*. Washington, DC: National Academy Press, 1992.
- Nelkin, Dorothy. "Behavioral Genetics and Dismantling the Welfare State." In *Behavioral Genetics: The Clash of Culture and Biology*, edited by Ronald A. Carson and Mark A. Rothstein, 156-158. Baltimore, MD: Johns Hopkins University Press, 1999.
- Nelkin, Dorothy, and Lori Andrews. "DNA Identification and Surveillance Creep." *Sociology of Health & Illness* 21, no. 5 (1999): 689-706. doi:10.1111/1467-9566.00179.
- Ng, Alfred. *Supreme Court Says Warrant Necessary for Phone Location Data in Win for Privacy: US Justices Say Law Enforcement Needs a Warrant to Follow Your Digital Footprints*. June 22, 2018. <https://www.cnet.com/news/supreme-court-says-warrant-necessary-for-phone-location-data/>.
- Norrgard, Karen. "Forensics, DNA Fingerprinting, and CODIS." *Nature Education* 1, no. 1 (2008): 35.
- Paoletti, David R., Travis E. Doom, Michael L. Raymer, and Dan E. Krane. "Assessing the Implications for Close Relatives in the Event of Similar but Nonmatching DNA Profiles." *Jurimetrics* 46 (2006): 161-175.
- Petti, David A. "An Argument for the Implementation of a Biometric Authentication System." *Journal of the Patent and Trademark Office Society* 80 (1998): 726-7.
- "People v. Anthony Ayler." *New York Law Journal*, October 1, 2004.
- "Peyton Manning Not Looking." n.d. <http://www.usatoday.com>.
- Pollack, Andrew. "Is a DNA Scan a Medical Test or Just Informational? Views Differ." *New York Times*, March 19, 2010.

- Rao, Neomi. "Three Concepts of Dignity in Constitutional Law." *Notre Dame Law Review* 86, no. 1 (2013): 183.
- Rao, Radhika. "Property, Privacy and the Human Body." *Boston University Law Review* 80 (2000): 359-460.
- Rashbaum, William. "Man Cleared by DNA Tests Led Police to Murder Suspect." *New York Times*, August 8, 2001.
- Re, Richard M. "The Due Process Exclusionary Rule." *Harvard Law Review* 127, no. 7 (2014): 1885.
- Regalado, Antonio. "How US Experts Helped China Build a DNA Surveillance State." February 21, 2019. <https://www.technologyreview.com/f/613000/how-us-experts-helped-china-build-a-dna-surveillance-state/>.
- Riserus, Ulf, Walter C. Willett, and Frank B. Hu. "Dietary Fats and Prevention of Type 2 Diabetes." *Progress in Lipid Research* 48, no. 1 (2009): 44-51.
doi:10.1016/j.plipres.2008.10.002.
- Roewer, Lutz. "Male DNA Fingerprints Say More." *Promega Life Sciences Case Report*, August 2003. <https://www.researchgate.net/publication/237283457>.
- Roewer, Lutz, and Walther Parson. "Internet accessible population databases: YHRD and EMPOP." In *Encyclopedia of Forensic Sciences*, edited by Jay A. Siegel and Pekka J. Saukko, 357-364. Waltham, MA: Elsevier, 2013.
- Ross, Rachel. "A Trail of Genetic Evidence Follows Us All." *Toronto Star*, February 2, 2004.
- Rothman, Barbara Katz. *Genetic Maps and Human Imaginations: The Limits of Science in Understanding Who We Are*. New York: W. W. Norton, 1998.
- Rothstein, Mark A. "Genetic Stalking and Voyeurism: A New Challenge to Privacy." *University of Kansas Law Review* 57, no. 3 (2009): 539-578.
- Roush, Wade. "Conflict Marks Crime Conference." *Science* 269, no. 5232 (1995): 1808-1809. doi:10.1126/science.7569909.
- Saks, Michael J., and Jonathan J. Koehler. "The Coming Paradigm Shift in Forensic Identification Science." *Science* 309, no. 5736 (2005): 892-895.
doi:10.1126/science.1111565.

- Sankar, Pamela. "DNA-Typing: Galton's Eugenic Dream Realized." In *Documenting Individual Identity: The Development of State Practices in the Modern World*, edited by Jane Caplan and John Torpey, 223-230. Princeton, NJ: Princeton University Press, 2001.
- Saplakoglu, Yasemin. *How the Golden State Killer's DNA Nabbed Him*. April 26, 2018. <https://www.livescience.com/62421-golden-state-killer-dna-genealogy.html>.
- Scherr, Albert E. "Genetic Privacy and the Fourth Amendment: Unregulated Surreptitious DNA Harvesting." *Georgia Law Review* 47 (2013): 445-526.
- Schneider, Harvey A. "Katz v. United States: The Untold Story." *McGeorge Law Review* 40, no. 1 (2008): 13-23.
- Schultz, Susanne. "Stop the DNA Collection Frenzy!": Expansion of Germany's DNA Database. 2014. <http://dnapolicyinitiative.org/genewatch-forensic-dna/stop-the-dna-collection-frenzy-expansion-of-germanys-dna-database/>.
- Schweigert, Keith. "Raymond Rowe, the Ex-DJ Accused in Christy Mirack Murder Case, Waives Preliminary Hearing." July 23, 2018. <https://fox43.com/2018/7/23/raymond-rowe-the-ex-dj-accused-in-christy-mirach-murder-case-waives-preliminary-hearing/>.
- Schwinn, Steven D. "Fourth Amendment: Preview of United States Supreme Court Cases." *American Bar Association* (2013): 215.
- Shapiro, Ari. *Police Use DNA to Track Suspects through Family*. December 12, 2007. <https://www.npr.org/templates/story/story.php?storyId=17130501>.
- Shapiro, Emily. *DNA on Gum, Water Bottle Leads to DJ's Arrest 26 Years after Teacher Killed*. June 26, 2018. <https://abcnews.go.com/US/dna-gum-water-bottle-leads-djs-arrest-26/story?id=56165384>.
- Simmons, Ric. "From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies." *Hastings Law Journal* 53, no. 6 (2002): 1303-1358.
- Simoncelli, Tania, and Barry Steinhardt. "California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases." *Journal of Law, Medicine & Ethics* 34, no. 2 (2006): 199-213. doi:10.1111/j.1748-720X.2006.00027.x.
- Skloot, Rebecca. "Taking the Least of You." *New York Times Magazine*, April 16, 2006.

- Slobogin, Christopher. *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*. Oxford: Oxford University Press, 2007.
- Slobogin, Christopher. "Public Privacy: Camera Surveillance of Public Places and The Right to Anonymity." *Mississippi Law Journal* 72 (2002): 213.
- Slobogin, Christopher, and Joseph E. Schumacher. "Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings' Recognized and Permitted by Society." *Duke Law Journal* 42 (1993): 727-775.
- Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: President and Fellows of Harvard College, 2008.
- Solove, Daniel J., and Paul M. Schwartz. *Information Privacy Law*. 5th ed. New York: Wolters Kluwer Law & Business, 2014.
- Springer Nature. *Open Reading Frames*. 2019. <https://www.nature.com/subjects/open-reading-frames>.
- Sullivan, J. "DNA on Envelope Sealed Man's Conviction in '82 Murder: Now He'll Go Free." *Seattle Times*, February 2, 2011.
- Sweet, David, and Gary G. Shutler. "Analysis of Salivary DNA Evidence from a Bite Mark on a Body Submerged in Water." *Journal of Forensic Sciences* 44, no. 5 (1999): 1069-1072. doi:10.1520/JFS12045J.
- The Tech Museum of Innovation. *Mutations and Disease*. 2013. <https://genetics.thetech.org/about-genetics/mutations-and-disease>.
- Thompson, Richard S. "The Fourth Amendment Third-Party Doctrine." *Congressional Research Service*, June 5, 2014. <https://fas.org/sgp/crs/misc/R43586.pdf>.
- Totenburg, Nina. "In Major Privacy Win, Supreme Court Rules Police Need Warrant to Track Your Cellphone." *NPR*, June 22, 2018. <https://www.npr.org/2018/06/22/605007387/supreme-court-rules-police-need-warrant-to-get-location-information-from-cell-to>.
- Touchette, Nancy. "Genome Test Nets Suspected Serial Killer." *Genome News Network*, June 13, 2003. http://www.genomenewsnetwork.org/articles/06_03/serial.shtml.

- U. N. Human Rights Committee. "Concluding Observations: Kuwait." 2000.
<https://www.refworld.org/publisher,HRC,CONCOBSERVATIONS,KWT,3df36be44,0.html>.
- U. S. Congress, Office of Technology Assessment. *New Developments in Biotechnology: Ownership of Human Tissues and Cells*. Special Report, Washington, DC: U. S. Government Printing Office, 1987.
- U.S. Congress, Office of Technology Assessment. *Genetic Witness: Forensic Uses of DNA Tests, OTA-BA-438*. Washington, DC: U.S. Government Printing Office. 1990.
- U.S. Department of Justice, Office of Justice Programs. *Using DNA to Solve Cold Cases*. Washington, DC: Author, 2002.
- Vacic, Vladimir, Shane McCarthy, Dheeraj Malhotra, Fiona Murray, Hsun-Hua Chou, Aine Peoples, Vladimir Marakov, et al. "Duplications of the Neuropeptide Receptor Gene VIPR2 Confer Significant Risk for Schizophrenia." *Nature* 471, no. 7339 (2011): 499-503. doi:10.1038/nature09884.
- van Derbeken, Jason. "How Alleged Serial Killer Fell into Trap." *San Francisco Chronicle*, September 21, 2003.
- van Oorschot, Roland, and Maxwell K. Jones. "DNA Fingerprints from Fingerprints." *Nature* 387 (1997): 767.
- Vladeck, Stephen. *The Supreme Court Phone Location Case Will Decide the Future of Privacy*. June 16, 2017. https://www.vice.com/en_us/article/59zq5x/scotus-cell-location-privacy-op-ed.
- Wade, Nicholas. "Unusual Use of DNA Aided in Serial Killer Search." *New York Times*, June 3, 2003.
- Warren, Samuel, and Louis Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.
- Wee, Sui-Lee. "China Uses DNA to Track Its People, With the Help of American Expertise." *New York Times*, February 21, 2019.
- Wenzel, Rainer. *ENFSI: Report on Criminal Cases in Europe Solved by ILS (DNA Mass Testing)*. 2016. http://enfsi.eu/wp-content/uploads/2016/09/enfsi_report_on_criminal_cases_in_europe_solved_by_ils_0.pdf.

- Wertz, Dorothy C., John C. Fletcher, Kare Berg, Victor Boulyjenkov, and World Health Organization. *Guidelines on Ethical Issues in Medical Genetics and the Provision of Genetics Services*. Geneva: World Health Organization, 1995.
- Wessler, Nathan F. *The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In*. June 28, 2019. <https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-most-consequential-ruling-privacy-digital> .
- White, Douglas, Donna Buckingham, Belinda Clark, and Helen McQueen. "The Use of DNA in Criminal Investigations." *Issues Paper | He Puka Kaupapa* 43 (2018). <https://lawcom.govt.nz/sites/default/files/projectAvailableFormats/DNA%20IN%20CRIMINAL%20INVESTIGATIONS%20-%20IP43%20-%20Final.pdf>.
- Wiegand, Peter, Thomas Bajanowski, and Bernd Brinkman. "DNA Typing of Debris from Fingernails." *International Journal of Legal Medicine* 106, no. 2 (1993): 81-83. doi:10.1007/BF01225045.
- Williamson, Robert, and Rory Duncan. "Commentary: DNA Testing for All." *Nature* 418 (2002): 585-6.
- Willing, Richard. "As Police Rely More on DNA, States Take a Closer Look." *USA Today*, June 6, 2000.
- . "Authorities Find More Uses for DNA Databases." *USA Today*, March 26, 2007.
- . "DNA's Success in Crime-Fighting Spread Unevenly." *USA Today*, October 6, 2002.
- . "Local DNA Labs Avoid State and U.S. Limits: Databases Nab Criminals, but Legality in Question." *USA Today*, March 26, 2007.
- . "Police Dupe Suspects into Giving up DNA." *USA Today*, September 11, 2003.
- Wilson, Mark R, Deborah Polanskey, John Butler, Joseph A. DiZinno, Jeri Replogle, and Bruce Budowle. "Extraction, PCR Amplification and Sequencing of Mitochondrial DNA from Human Hair Shafts." *BioTechniques* 18, no. 4 (1995): 662-669.
- Wright, Clayton E., Barbara J. Evans, James W Hazel, and Mark A. Rothstein. "The Law of Genetic Privacy: Applications, Implications, and Limitations." *Journal of Law and the Biosciences* (2019): 1-36. doi:10.1093/jib/lisz007.

Yamine, Evelyn. "How a Hand-Rolled Cigarette Led Police to a Murder Charge." *Daily Telegraph*, September 24, 2004.

Yasuda, Toshihiro, Reiko Iida, Haruo Takeshita, Misuzu Ueki, Tamiko Nakajima, Yasushi Kaneko, Kouichi Mogi, Tetsuya Tsukahara, and Koichiro Kishi. "A Simple Method of DNA Extraction and STR Typing from Urine Samples Using a Commercially Available DNA/RNA Extraction Kit." *Journal of Forensic Sciences* 48, no. 1 (2003): 108-110. doi:10.1520/JFS2002184.

Zimmerli, Walther C. "Who Has the Right to Know the Genetic Constitution of a Particular Person?" *Ciba Foundation Symposium* 149 (1990): 93-110.