
GETTING IT RIGHT: LAW ENFORCEMENT’S USE OF ANCESTRY
WEBSITES TO CATCH CRIMINALS

Mackenzie L. Brockmyre*

I. Introduction

For the past thirty years, deoxyribonucleic acid (“DNA”) evidence has been the gold standard in forensic science to solving criminal cases.¹ The advent of DNA use in the late 1980’s opened a world of possibilities previously unavailable to investigators.² Prior

* J.D. Candidate, Suffolk University Law School, 2021; BS, Business Administration in Accounting, University of Richmond, 2011. Mackenzie can be reached at mac.brockmyre@gmail.com.

¹ See Celia Henry Arnaud, *Thirty years of DNA forensics: How DNA has revolutionized criminal investigations*, C&EN (Sept. 18, 2017), archived at <https://perma.cc/79DE-6HJL> (stating that since the first criminal case was solved in 1987, DNA has become the “gold standard in forensic science”). While forensic lab backlogs cause processing delays, the process to retrieve DNA samples has become more precise and requires less material. *Id.* See Randy James, *A Brief History of DNA Testing*, TIME (June 19, 2009), archived at <https://perma.cc/QVN6-XAF9> (explaining that the use of DNA is the most reliable physical evidence available to investigators). One of the best tools available to criminalists prior to DNA was the use of “blood typing.” *Id.* RICHARD SAFERSTEIN, *FORENSIC SCIENCE FROM THE CRIME SCENE TO THE CRIME LAB*, 371 (2d ed. 2013) (explaining that scientists have identified more than one hundred blood factors used in blood typing, which if properly identified at a crime scene, can link a suspect to a crime). Determining that the use of blood typing has been replaced in favor of DNA evidence, which carries the body’s genetic information. *Id.*

² See Ian Cobain, *Killer breakthrough—the day DNA evidence first nailed a murderer*, THE GUARDIAN (June 8, 2016), archived at <https://perma.cc/4EPA-4VWP> (according to estimates, more than fifty million people have submitted DNA

to this revelatory discovery, the public perceived crime scene investigations as little more than conjecture.³ Of course there was more to the methodology than purely educated guesses; nonetheless, there is a long history of individuals that were incarcerated and have hence been exonerated by the use of DNA.⁴ Using DNA to solve cases, notably those involving sexual assault, is becoming more prevalent because of decreasing costs and improved accuracy of test results.⁵

pursuant to criminal investigations and it has possibly convicted millions). *See also* James, *supra* note 1 (highlighting the fact that forensic testing using DNA has better than 99% accuracy when matching genetic material found at a crime scene to the perpetrator). New techniques allow authorities to collect and analyze smaller amount of DNA as technology evolves. *Id.* *See Using DNA to Solve Cold Cases*, NAT'L INST. OF JUST. (July 2002), *archived at* <https://perma.cc/2CFS-DCNK> (detailing the use of DNA evidence as a powerful tool because it can be collected from almost every cell in the human body, which if properly preserved, can be used to solve old cases).

³ *See* Penny Bailey, *Before DNA: 20th-century forensics*, PHYS.ORG (Sept. 6, 2011), *archived at* <https://perma.cc/84TF-W8SK> (“We tend to think that before Alec Jeffries’ eureka moment in 1984, when he realized that genetic variations in DNA could identify individuals, crime investigations were really just guesswork.”). The change in criminologists date back to “celebrity pathologists” to a “manager of routine, tedious, laboratory work.” *Id.* The belief that crime scene investigators lacked credibility before DNA testing is false because the concerns about crime scene management and integrity, chain of custody, and interpreting trace evidence were “live concerns” long before. *Id.*

⁴ *See id.* (defending early criminology by stating that conventional autopsy processes evolved into complex trace analysis that demanded specialized knowledge and equipment). *See DNA Exonerations in the United States*, INNOCENCE PROJECT (Oct. 5, 2019), *archived at* <https://perma.cc/3CBJ-WJP6> (giving statistics on DNA exonerations in the United States, with the first one taking place in 1989). A quarter of exonerations in the United States have been due to the use of DNA evidence. *Id.* *See also* Emily Barone, *The Wrong Convicted: Why more falsely accused people are being exonerated today than ever before*, TIME (Oct. 18, 2019), *archived at* <https://perma.cc/3KRB-LPP7> (particularizing wrongful conviction issues to perjury, false identifications, and racial bias stemming from law enforcement practices); James, *supra* note 1 (emphasizing the fact that while genetic matches are extraordinarily reliable in convicting criminals, DNA testing is “virtually foolproof in exonerating the innocent”).

⁵ *See* James, *supra* note 1 (noting that DNA analysis is becoming more widespread and kits can even be purchased at drugstores). Biological material such as skin, hair, blood, and other bodily fluids can be collected from common items that a criminal may have touched briefly. *Id.* DNA use has even crossed into sports, as footballs used in the Super Bowl are marked with DNA to prevent counterfeiting. *Id.* Stating that “there’s just a 1 in 33 trillion chance of getting the pigskins” genetic sequence right. *Id.* (emphasis added). *See also* Saferstein, *supra* note 1, at

DNA use since its inception has influenced criminal investigations in a way as groundbreaking as the Industrial Revolution's impact on advancement in modern society.⁶ As Modern society moves beyond the Second, and even Third Industrial Revolution ("Digital Revolution"), into the midst of a so-called "Fourth Industrial Revolution" headlined by artificial intelligence and autonomous cars, DNA evidence will continue to evolve.⁷ These

384 (explaining that new technology has allowed for increased sensitivity of DNA analysis, which has created new areas of investigation including linking a victim and an assailant by analyzing biological material recovered from underwear). This is development in collection methods has proven especially important in sexual assault cases when suspect's DNA cannot be recovered from the victim. *Id.* See also Jennifer Graddy, *The Ethical Protocol for Collecting DNA Samples in the Criminal Justice System*, 59 J. OF MOLECULAR BIOLOGY 226, 227 (2003) (estimating that 30% of sexual assault victims cannot identify their attackers, however, "[m]iniscule amounts of DNA recovered from a crime scene can be used to link an otherwise [unidentified] suspect to the crime").

⁶ See *Economic Growth and the Early Industrial Revolution*, U.S. HISTORY: PRE-COLUMBIAN TO THE NEW MILLENNIUM (Oct. 5, 2019), archived at <https://perma.cc/3JGK-B6AQ> (explaining that the shift from agriculture to machine-made products during the industrial revolution created a higher standard of living than had ever been known in human history). It should be acknowledged that the Industrial Revolution had well documented humanitarian issues at the expense of the working class while the rich got richer, however, there is reliable statistical evidence showing that the working class, as a whole, realized higher wages, more food, and better clothing. *Id.*

⁷ See Goncalo de Vasconcelos, *The Third Industrial Revolution—Internet, Energy And A New Financial System*, FORBES (Mar. 4, 2015), archived at <https://perma.cc/7D69-EVL6> (describing the Second Industrial Revolution as the modernization of society through mass electricity, the telephone, the internal combustible engine, and new ways of doing business such as the limited liability company). Beginning with the tech boom and bust in the mid-90s, the internet has risen and impacts "eventually everything" in the Third Industrial Revolution. *Id.* See also Paul Hudson, *Why The Tech Revolution Is The Industrial Revolution Of Our Time*, ELITE DAILY (Mar. 29, 2013) (detailing how the Digital age has seen communication grow at an exponential rate from 1990 to 2010: cell phone subscribers rose from 12.4 million to 4 billion people; and internet usage went from 2.8 million to 1.8 billion people). See also Elizabeth Schulze, *Everything you need to know about the Fourth Industrial Revolution*, CNBC (Jan. 17, 2019), archived at <https://perma.cc/M9EZ-Y5VZ> (arguing that a new technological revolution is underway, which is "blurring the lines between the physical, digital, and biological spheres" and these three worlds are shrinking as technology is changing faster than ever). To put it plainly, the Fourth Industrial Revolution refers to technology such as voice-activated assistants, facial ID recognition or digital health-care sensors. *Id.*

technological innovations and countless more all advance at a break-neck pace, leaving people and companies behind.⁸ Consequently, those legislative bodies who make the law, and the judiciary who interpret it are on an even greater curve when it comes to catching up to technological changes in society.⁹ Nevertheless, the courts are trying to adapt to the changing times.¹⁰

⁸ See Schulze, *supra* note 7 (arguing companies and individuals that lack the necessary skills to analyze data will fall by the wayside, while rewarding high skilled workers and leaving lower-skilled workers behind). To exemplify how quickly technology is spreading, Zvika Krieger points out, “[i]t took 75 years for 100 million people to get access to the telephone; the gaming app “Pokemon Go” hooked that many users in less than one month in 2016.” *Id.* See also Vivek Wadhwa, *Laws and Ethics Can’t Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), archived at <https://perma.cc/238J-AZZ7> (explaining that a full human genome sequence cost \$100 million in 2002 and today only costs \$1,000). To further the point that technology has moved at a pace that puts the average person behind a substantial curve:

Not long ago, Facebook was a dorm-room dating site, mobile phones were for the ultra-rich, drones were multimillion-dollar war machines, and supercomputers were for secret government research. Today, hobbyists can build drones and poor villagers in India access Facebook accounts on smartphones that have more computer power than the Cray 2—a supercomputer that in 1985 cost \$17.5 million and weighed 2,500 kilograms.

Id. Offering that genome testing may soon become a commodity for businesses and there are few limits on commercial entities on using aggregated genomic data. *Id.* See also *Over 50 Years of Moore’s Law*, INTEL (Oct. 18, 2019), archived at <https://perma.cc/NW7X-9L2A> (explaining that Gordon Moore hypothesized that computing would dramatically increase in power and decrease in cost, at an exponential pace); *Top five social media privacy concerns*, REPUTATION DEFENDER (Jan. 24, 2018), archived at <https://perma.cc/6HPF-RS5D> (analyzing the risks of social media and how the user’s privacy is affected).

⁹ See Wadhwa, *supra* note 8 (explaining that regulatory gaps exist “because laws have not kept up with advances in technology”).

¹⁰ See David P. Fidler, *The Supreme Court Adapts Constitutional Law to Address Technological Change*, COUNCIL ON FOREIGN REL. (July 11, 2018), archived at <https://perma.cc/NB3G-GQ2L> (rejecting a mechanical application of a person’s reasonable expectation of privacy about one’s location generated by cellphones, because cellphone devices “have become indispensable in modern society”); see also Daniel Malan, *The Law can’t keep up with the new tech. Here’s how to close the gap*, WORLD ECON. FORUM (June 21, 2018), archived at <https://perma.cc/AJ2C-6AC9> (positing that the advances in technology are almost impossible to define with specificity, which would allow legislatures to catch up); David D. Friedman, *Does Technology Require New Law?*, 25 HARV. J. L. & PUB. POL’Y 71, 85 (2001) (stating that broad legal principles cannot be applied with predictable results at a reasonable cost and “new law” needs to be created to deal with new technologies);

This delay in how the law catches up to societal reality is displayed in the advancement of law enforcement's use of DNA, and how the judiciary views it from an evidentiary and constitutional perspective. This Note reflects on one of the most recent trends in DNA use in criminal investigations: law enforcement, on the state and federal levels, using DNA collected through "genealogy websites", such as www.ancestry.com and www.23andme.com, to match DNA collected at crime scenes to suspects. There is little debate surrounding consensual submissions of DNA to these databases. However, the motivating issue is whether those who do not submit their DNA to the websites have legal recourse if they are connected to a crime through such investigatory methodology. Foundationally, this Note explores the rise of DNA in the criminal justice system and how the law has treated it over the years. Part II discusses the explosion of genealogy websites and how law enforcement uses these websites to their advantage in creating "DNA trees" to indict and obtain convictions. In a culmination of the preceding topics, Part III discusses the facts surrounding the contemporary issues of law in discussing how legislatures and judiciaries at the state and federal levels are grappling with this new phenomenon. Finally, Part IV analyzes the right of privacy that third parties have to their personal, genetic material. This Note concludes that law enforcement should have the right to access genealogy websites for the purpose of comparing DNA found at crime scenes.

Carpenter v. U.S., 138 S.Ct. 2206, 2209 (2018) (holding that the government's use of cell-site records was a search under the Fourth Amendment). *See also* Commonwealth v. Serge, 896 A.2d 1170, 1178 (PA. 2006) ("The law does not, and should not, prohibit proficient professional employment of new technology in the courtroom. This is, after all, the twenty-first century").

II. History

A. *From Bloody Fingerprints to the Human Genome: The Rise of DNA and its use in Criminal Investigations*

1. A Brief History of Fingerprinting and Blood Analysis

Fingerprints have long been held as a way to identify a person.¹¹ Each individual touts prominent features on their hands and feet, which leave behind unique impressions when an object is touched.¹² Fingerprints have obviously existed as long as humans, and their use as a tool for purposes of identification stem from ancient times.¹³ However, it was not until the late 1800s that fingerprints were established as individually unique and wholly persistent among the population.¹⁴ Following society's acceptance of fingerprints as unique identifiers, this evidence made its way into the courtroom, exemplified by one of the first murder convictions using

¹¹ See Jeffery G. Barnes, *The Fingerprint Sourcebook*, NAT'L INST. OF SCI., 1:7 (Oct. 19, 2019), archived at <https://perma.cc/6NZL-TBAQ> (explaining that fingerprints have been used to identify people possibly as far back as 300B.C.).

¹² See *A Simplified Guide to Fingerprint Analysis*, FORENSIC SCI. SIMPLIFIED (2013), archived at <https://perma.cc/HH9T-6BYR> (describing the three ways to classify fingerprints: (1) fingerprints on soft surfaces that will be three-dimensional; (2) visible prints that are formed when blood, dirt, or another substance is transferred from a finger or thumb to a surface; (3) and invisible print, which can be found on a wide variety of porous and nonporous surfaces).

¹³ See Barnes, *supra* note 11, at 1:8 (stating that the ancient Chinese were the first known culture to use fingerprints as a means of identifying authors of documents by pressing fingerprints into clay seals of bamboo slips); see Barnes, *supra*, at 1:9 (demonstrating the use of fingerprints by Indian Royalty in the 1600s).

¹⁴ See *History of Fingerprints*, CRIME SCENE FORENSICS (2018), archived at <https://perma.cc/25MP-SDES> (noting that Sir Francis Galton was the first to publish a book on fingerprints, highlighting their uniqueness and individuality, which are known as "Galton Details"). In 1891, an Argentinian police official, Juan Vucetich, used a fingerprint found on a doorpost to identify and convict a woman who had killed her two children and attempted to blame another individual. *Id.* See also Chantel Tattoli, *The Surprising History (and Future) of Fingerprints*, THE PARIS REV. (May 15, 2018), archived at <https://perma.cc/6XXG-Z4EV> (arguing that real-world application of fingerprinting for forensic application would be problematic due to lack of a classification and index-system for decades). See also Barnes, *supra* note 11, at 1:13 (identifying this Argentinian case to be the first to rely solely on fingerprints as a method to distinguish suspects and the first homicide solved by fingerprint evidence).

fingerprint evidence in Chicago in 1910.¹⁵ This new form of evidence was met with fervent criticism as to its efficacy and reliability by defense attorneys.¹⁶ While fingerprinting has taken on a significant role in the United States law enforcement and judicial system, contention still surrounds potential deficiencies and shortcomings.¹⁷

¹⁵ See Francine Uenuma, *The First Criminal Trial That Used Fingerprints as Evidence*, SMITHSONIAN (Dec. 5, 2018), archived at <https://perma.cc/X8RC-ZML9> (recounting that the defendant, Jennings, had left behind a fingerprint from a freshly painted railing that he had touched upon exiting the home of the man he had just murdered). The defendant broke into the victim's home, a scuffle ensued, and the defendant allegedly shot a man before fleeing the scene. *Id.* The police photographed the railing where the fresh print was made, and this fingerprint was used at the trial as the main piece of evidence that led to his eventual conviction. *Id.*

¹⁶ See Barnes, *supra* note 11, at 1:17 (stating that Jennings appealed the case, claiming that the fingerprint evidence was improperly admitted, and the testimonies of the fingerprint experts were not necessary); Uenuma, *supra* note 15 (highlighting that the new technique for obtaining fingerprints was not understood, and that Britain had to create a special law to even use fingerprints in criminal proceedings). Upon appeal, the court held that fingerprint identification is indeed a science and that expert testimony was appropriate to aid the court. See Barnes, *supra* note 11, at 1:17.

From the evidence in this record we are disposed to hold that the classification of finger-print impressions and their method of identification is a science requiring study. . . the evidence in question does not come within the common experience of all men of common education in the ordinary walks of life, and therefore the court and jury were properly aided by witnesses of peculiar and special experience on this subject.

People v. Jennings, 96 N.E. 1077, 1083 (Ill. 1911). See also Mark A. Acree, *People v. Jennings: A Significant Case In American Fingerprint History*, SOUTHERN CAL. ASS'N OF FINGERPRINT OFFICERS (1998), archived at <https://perma.cc/H5HA-6W5N> (explaining this case's ruling legitimized fingerprint identification in the legal system, which is further evidenced by the frequency the case is cited to this day).

¹⁷ See *Fingerprints: The First ID*, FINDLAW (Oct. 19, 2019), archived at <https://perma.cc/LK6W-BT3K> (detailing how the FBI established a fingerprint database in 1924, which was followed by the Automated Fingerprint Identification System (AFIS) in 1991, which computerized the old card system). Criminals are fingerprinted when they are processed, but civil fingerprints are kept as well for people who apply for government jobs, jobs that require security clearance, teaching positions, and law enforcement positions. *Id.* See also Jamie Walvisch, *Fingerprinting to solve crimes: not as robust as you think*, THE CONVERSATION

In addition to fingerprint analysis, criminal investigations have historically relied on blood factor analysis called “blood-typing”.¹⁸ However, when criminologists and forensic scientists began analyzing blood types for investigative purposes, they quickly ran into issues rendering “blood-typing” as largely ineffective.¹⁹ The advent of DNA technology saved the statistical deficiencies of blood typing that plagued the legal system.²⁰ In 1984, the world changed when Dr. Alec Jeffreys, quite accidentally, discovered that repetitive patterns of DNA present in every human being varied for

(Oct. 23, 2017), *archived at* <https://perma.cc/S5KU-MQLW> (examining the validity of fingerprint identification, the President’s Council of Advisors on Science and Technology (PCAST) found that only *two* properly designed studies of invisible fingerprint analysis had been done, yielding false matches of “1 in 18,” and “1 in 30,” which is considered to be very high). The primary reason for the high error rates is because fingerprint analysis involves human judgment and relies on methodology that is not sufficient to ensure accuracy and reliability. *Id.* The error rate was discovered because DNA analysis is the only forensic method that has been rigorously validated. *Id.*

¹⁸ See Saferstein, *supra* note 1 (setting forth Karl Landsteiner’s discovery of “blood typing” in 1901, which evolved into the classification system that we refer to as the “A-B-O” system). Until the 1990s, forensic scientists focused on this classification system for the best method of linking blood at a crime scene to a suspect. *Id.* See *generally Evidence And Tools Used In Forensic Science*, FORENSIC SCI. (Oct. 19, 2019), *archived at* <https://perma.cc/7TMA-SSS8> (detailing how blood typing is used in solving criminal investigations).

¹⁹ See Randolph N. Jonakait, *Will Blood Tell Genetic Markers in Criminal Cases?*, 31 EMORY L. J. 833, 834 (1982) (concluding that a bloodstain at a murder scene matched the defendant’s blood, and only one in a thousand people have the same blood type). See also Corey Harbison, *ABO Blood Type Identification and Forensic Science (1900-1960)*, THE EMBRYO PROJECT ENCYCLOPEDIA (June 2, 2016), *archived at* <https://perma.cc/Y5WK-5XK3> (describing that blood typing could be helpful to prove innocence, but could not be used accurately to identify a suspect beyond a reasonable doubt). By the 1960’s, scientists could exclude individuals based on blood samples, but they could only give statistical probabilities to *include* people as the source of a blood sample found at a crime scene. *Id.*

²⁰ See Harbison, *supra* note 19 (conceding that legislatures began allowing courts to order witnesses in criminal trials to submit to compulsory blood group testing, which proved controversial); see also *Blood Typing And The Abo Groupings*, DNA PROFILING (Oct. 19, 2019), *archived at* <https://perma.cc/M44W-USLS> (recognizing that most court cases rely on more evidence than just blood or DNA typing); Saferstein, *supra* note 1 (underscoring the shift from searching for genetically controlled blood factors in bloodstains was abandoned in favor of “characterizing biological evidence by select regions in our deoxyribonucleic acid (DNA), which carries the body’s genetic information.”).

each individual, thus ushering in the technique known as “DNA fingerprinting”.²¹

2. DNA’s Ascension and how the Law Grappled with the Technological (R)Evolution

DNA was first discovered in 1869; however, there was no knowledge of how it functioned until the early 1950’s when James Watson and Francis Crick discerned the substance’s structure.²² Watson and Crick’s discovery led to Dr. Jeffreys’ accidental realization that DNA can differentiate between two individuals with 99% accuracy in 1984.²³ Shortly after Dr. Jeffreys showed the world

²¹ See *DNA Fingerprinting—The Discovery of DNA Fingerprinting*, DNA FORENSICS (Oct. 19, 2019), archived at <https://perma.cc/K6XC-UW48> (establishing that while Dr. Jeffreys was studying hereditary diseases in families, he discovered repetitive patterns of DNA called “Variable Number of Tandem Repeats” (VNTRs) that were present in all humans but they varied in length in each person). VNTRs became known as a “genetic fingerprint”, which is specific to each individual and does not belong to another person, except for identical twins. *Id.* See also *The science behind genetic fingerprinting*, UNIV. OF LEICESTER (Oct. 19, 2019), archived at <https://perma.cc/P9E4-4YXZ> (stating Dr. Jeffreys’ discovery has had a dramatic impact in criminal investigations and is known as one of the most impactful discoveries in human molecular genetics).

²² See *DNA and proteins are key molecules of the cell nucleus*, DNA FROM THE BEGINNING (Oct. 20, 2019), archived at <https://perma.cc/UK4X-393C> (stating that Friedrich Miescher first discovered a molecule called nuclein from a cell’s nucleus that he believed were the proteins that were the molecules of heredity, but it would be years before the roles of nucleins were recognized); see also Joseph L. Schwartz, Comment, *Evidence—The Admissibility of Statistical Probabilities in DNA Testing for Suspect Identification in Criminal Proceedings—Commonwealth v. Curnin*, 409 Mass. 218, 565 N.E.2d 440 (1991), 25 SUFFOLK UNIV. L. REV. 868, 870 (1991) (elucidating that DNA is found within the nucleus of every cell in the body that contains an individual’s genetic makeup).

²³ See *The science behind genetic fingerprinting*, *supra* note 21 (identifying that Dr. Jeffreys used a method known as “Restricted Fragment Length Polymorphism” (RFLP) to analyze DNA to try and resolve paternity and immigration disputes). This method led him to discover that the RFLP variation resulted in alterations in bases in our DNA, and we now know there are about 10 million different sites at which individuals can vary their DNA sequence. *Id.* Importantly, he also showed some regions of DNA, which are termed “minisatellites,” showed stuttered patterns, but were variable within the stutters and were the basis for DNA fingerprinting. *Id.* Compare James, *supra* note 1 (highlighting the fact that forensic testing using DNA has better than 99% accuracy), with Jonakait, *supra*

the power of DNA, he was asked to assist with two seemingly connected crimes.²⁴ There were three important outcomes from these cases: (1) the same killer was responsible for both crimes, even though the crimes happened three years apart; (2) DNA was able to exonerate an innocent man even after he had confessed to the crimes; and most importantly (3) DNA was able to identify the person responsible for the crimes.²⁵ Interestingly, this research introduced the concept of DNA “dragnets”, which have been replaced by government and direct-to-consumer (“DTC”) computerized databases.²⁶ However, the legality of the DNA evidence was not

note 19 (juxtaposing the relative inaccuracy of blood-typing, which narrows down a hypothetical suspect to one in one thousand).

²⁴ See *The Discovery of DNA Fingerprinting*, *supra* note 21 (discussing that in 1983, a 15-year old girl was raped and murdered and three years later, another 15-year old girl was raped and murdered in Leicestershire, England). A 17-year-old boy with learning disabilities confessed to the rape and murder of the second girl, however, Dr. Jeffreys tested the accused boy’s blood with the semen taken from the decedent’s bodies and found that they had been raped by the same man, and that the accused’s DNA was completely different. *Id.* See also Cobain, *supra* note 2 (highlighting the fact police thought they had the right suspect, especially since he had confessed to the crimes).

²⁵ See Cobain, *supra* note 2 (explaining that DNA had proven the detective’s original theory correct that one suspect, Colin Pitchfork, murdered both girls, who avoided having his blood taken when police solicited samples from every male born between 1953 and 1970); see also *The Discovery of DNA Fingerprinting*, *supra* note 21 (detailing Colin Pitchfork’s ploy, was later discovered by law enforcement). When police confronted Pitchfork about his involvement, he immediately confessed and plead guilty, and his guilt was confirmed when Dr. Jeffreys compared Pitchfork’s DNA to the semen on the two victims. *Id.*

²⁶ See Cobain, *supra* note 2 (stating that police used a screening process to gather blood samples from every man of a certain age in the area). Over a period of eight months, 5,511 men had given blood samples and this “dragnet” search for matching DNA had garnered international attention. *Id.* These mass dragnets, which have been conducted occasionally across the globe, have been largely abandoned in favor of national DNA databases that were established in the 1990s, because they do not have the human element of avoidance that was demonstrated in the Pitchfork case. *Id.* See also Mark Hansen, *DNA Dragnet*, ABA JOURNAL (May 1, 2004), archived at <https://perma.cc/634M-PGKA> (stating that since 2004, only one DNA dragnet has led directly to the identification of the actual perpetrator). Advocates stated that dragnets were similar to fingerprinting or drunk driving roadblocks, however, the effectiveness was always in question along with constitutional issues such as Fourth and Fifth Amendment right of privacy and self-incrimination violations, respectively. *Id.*

tested in the English court, leaving the new science's admissibility an open question both in England and the United States.²⁷

The first case to test the admissibility of DNA evidence, more specifically "genetic fingerprinting" was *Andrews v. Florida*, where the District Court of Appeals held that it was indeed admissible.²⁸ While this was a victory for prosecutors because it gave them a mighty tool to indict and convict criminals, the legal battle over the admissibility of DNA had only begun.²⁹ As courts began to grapple

²⁷ See Cobain, *supra* note 2 (concluding that because Pitchfork plead guilty to the crimes, the DNA evidence was not relied upon by prosecution and thus the science was not tested by the English courts); see also Lisa Calandro Dennis & J. Reeder Karen Cormier, *Evolution of DNA Evidence for Crime Solving—A Judicial and Legislative History*, FORENSIC MAG. (Jan. 6, 2005), archived at <https://perma.cc/K96K-YBTA> [hereinafter Dennis] (articulating that the judicial system has placed extensive scrutiny on DNA evidence over the years because of the relative novelty of the technology and methodology).

²⁸ See *Andrews v. State*, 533 So. 2d 841, 843 (Fla. Dist. Ct. App. 1988) (quoting "[w]e have found no other appellate decision addressing the admissibility of DNA identification evidence in criminal cases."). The court held:

In contrast to evidence derived from hypnosis, truth serum and polygraph, evidence derived from DNA print identification appears based on proven scientific principles. Indeed, there was testimony that such evidence has been used to exonerate those suspected of criminal activity. Given the evidence in this case that the test was administered in conformity with accepted scientific procedures so as to ensure the greatest degree possible a reliable result, appellant failed to show error on this point.

Id. at 850–51. See Dennis, *supra* note 27 (explaining that the appellate court affirmed the trial courts conviction after Andrews' DNA matched semen traces found in a rape victim).

²⁹ See *Commonwealth v. Curnin*, 565 N.E.2d 440, 442 (Mass. 1991) (identifying that during that time DNA test results were not admissible in court). The court stated that studies were underway to determine if DNA tests should have a role to play in proving the identity in criminal trials, highlighting that the problem is in deciding how the scientific concepts should be implemented. *Id.* at 442 (holding that "there is no demonstrated general acceptance or inherent rationality of the process" by which the lab that performed the test arrived at its conclusion that the defendant's DNA matched that found on the evidence at the crime scene); see also Schwartz, *supra* note 22, at 873 (expressing optimism for the future of DNA as of 1991 coupled with skepticism about the novelty of DNA testing and the methods used to arrive at the statistical probabilities in the *Curnin* case). Compare *Frye v. U.S.*, 293 F. 1013, 1014 (D.C. Cir. 1923) (holding that where the subject-matter is of a science, art, or trade which requires experience in order to acquire knowledge

with DNA testing, a new testing methodology emerged called “polymerase chain reaction” (“PCR”), inviting another round of challenges from defense attorneys.³⁰ Luckily, a string of cases in 2001 solidified PCR’s place in the courtroom by ruling the new process scientifically sound and admissible.³¹

Over the thirty years that DNA testing has been used in criminal cases, it is estimated that millions of convictions have been secured.³² Convictions have been obtained more efficiently by the institution of DNA databases, which made dragnets a thing of the past and enabled law enforcement to classify and store DNA obtained

of it and would not lie within the common experience or knowledge, the opinions of witnesses skilled in that particular area to which the question relates are admissible), and Dennis, *supra* note 27 (explaining that under *Frye*, in order for scientific evidence to be admissible it must be “sufficiently established to have gained general acceptance in the particular field in which it belongs.”), with *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 597 (1993) (holding that “general acceptance” is not a necessary precondition for scientific evidence to be admissible, but evidence based on scientifically valid principles will be admitted to assist the trier of fact). A summary of what courts needed to determine under the *Free* rule:

- (1) The status, in the appropriate scientific community, of the scientific principle underlying the proffered novel evidence;
- (2) the technique applying the scientific principle; and
- (3) the application of the technique on the particular occasion.

See 533 So. 2d at 843 (citing Giannelli, *The Admissibility of Novel Scientific Evidence: Frye v. United States A Half Century Later*, 80 COLUM. L. REV. 1197, 1201 (1980)).

³⁰ *See* Dennis, *supra* note 27 (noting the transition of methodology from RLFP to PCR using “short tandem repeats” (STRs) gave defense lawyers another crack at challenging the admissibility and reliability of DNA). PCR allows small quantities of DNA found at crime scenes to be copied or multiplied, which allows forensic scientists to gather miniscule amounts of evidence at a crime scene and create a usable sample for testing. *Id.* *See also* Saferstein, *supra* note 1, at 389 (reflecting on the forensic science practice of enzyme and protein manipulation during DNA replication for DNA identification purposes).

³¹ *See* *People v. Hill*, 107 Cal. Rptr. 2d 48, 60 (Cal. Ct. App. 2001) (accepting the use of PCR testing method because it is generally accepted by the scientific community and is more “sophisticated because it examines a greater number of genetic markers.”); *Lemour v. State*, 802 So. 2d 402, 408 (Fla. Dist. Ct. App. 2001) (holding that the PCR method is generally accepted by the scientific community and, even though the testing process failed to follow the Technical Working Group on DNA Analysis Methods (TWGDAM), the evidence and results are still admissible); *People v. Shreck*, 22 P.3d 68, 83 (Colo. 2001) (holding that DNA evidence derived from PCR testing is admissible).

³² *See* Cobain, *supra* note 2 (asserting that according to some estimates DNA has secured millions of convictions).

from prior offenders.³³ The federal DNA Identification Act of 1994 mandated the Combined DNA Index System (“CODIS”), which is handled by the FBI.³⁴ The Violent Crime Control and Law Enforcement Act was implemented the same year, and ensures uniform standards in the collection, analyzation and forensic testing of DNA.³⁵ The Justice for All Act of 2004 materially changed the DNA Identification Act of 1994 through expansion of the list of offenses for which federal samples are collected, enhancement of criminal penalties for unauthorized use of CODIS, and updated accreditation standards for labs.³⁶ In addition to CODIS, all fifty

³³ See Jessica D. Gabel, *Indecent Exposure: Genes Are More Than a Brand Name Label in the DNA Database Debate*, 42 U. BALT. L. REV. 561, 563 (2013) (noting that the police caught a serial rapist in 2012 after a sample in CODIS matched evidence from a twenty-five-year-old rape case). See also Graddy, *supra* note 5, at 226 (expounding on the benefits of DNA databases such as: using samples from databases to match samples found at crime scenes, establishing links between different crimes, and solving not old cold cases but future crimes as well); Martha L. Lawson, *Personal Does Not Always Equal “Private”*: *The Constitutionality of Requiring DNA Samples from Convicted Felons and Arrestees*, 9 WM. & MARY BILL RTS. J. 645, 649 (2001) (noting that the British DNA database, which has samples taken from all persons charged with a “recordable offense” since 1995, has helped to solve about 500 crimes per week). As of 2001 the newly created and operational federal database had been used to find over 400 matches with samples from crime scenes. *Id.* at 649–50.

³⁴ See 34 U.S.C.A. § 12592 (West 2017) (formerly cited as 42 U.S.C.A. § 14132(a) (West 2014)) (establishing the federal DNA database whereby the FBI may keep an index of DNA records of: persons convicted of crimes; persons who have charged in an indictment or information with a crime; and other persons whose DNA samples are collected under legal authorities; analyses of DNA samples recovered from crime scenes; analyses of DNA samples recovered from unidentified human remains; analyses of DNA samples voluntarily contributed from relatives of missing persons); Gabel, *supra* note 33, at 565 (describing what and where CODIS collects and stores); *Combined DNA Index System (CODIS)*, FBI (Oct. 6, 2019), archived at <https://perma.cc/Y9GG-QW8J> (establishing FBI’s CODIS as the original pilot program in 1990, serving fourteen state and local laboratories).

³⁵ See 34 U.S.C.A. § 12591 (West 2017) (formerly cited as 42 U.S.C.A. § 14131(West)) (mandating quality assurance and proficiency testing standards relating to DNA testing).

³⁶ See *Statement on Compliance with Laws and Regulations*, OFF. OF THE INSPECTOR GEN. (May 2006), archived at <https://perma.cc/V29J-VXTF> (delineating what the Act changed).

states maintain DNA databases.³⁷ The explosive growth of databases nationwide led to “cold hits”, where no suspect has been identified, but evidence from crime scenes are matched to databases that resulted in a match from a previously convicted criminal.³⁸ Legislatures, recognizing the potential of databases to assist law enforcement, began to authorize “John Doe” or “DNA” warrants, which are not issued for a particular person, but for a particularized genetic code.³⁹

An ancillary, and what would hopefully be unintended consequence of establishing national databases, such as CODIS, is the racial disparity of the stored information.⁴⁰ Based on a Bureau of Justice statistical model, a young black man in 1996 had a 28.5

³⁷ See Gabel, *supra* note 33, at 565 (stating that all fifty states have instituted similar provisions that establish DNA databases, while some states expanded the list of criminals to include sexual and violent offenders and those convicted of misdemeanors); *see id.* at 565–66 (noting that states have also started following the federal practice of collecting samples from arrestees, not just convicted criminals); Graddy, *supra* note 5 (stating that Virginia became the first state to create a criminal DNA database in 1989); *DNA Data Bank*, VIRGINIA DEP’T OF FORENSIC SCI. (Oct. 6, 2019), *archived at* <https://perma.cc/57KR-24HH> (detailing the milestones of Virginia’s DNA Data Bank program).

³⁸ See Ranajit Chakraborty & Jianye Ge, *Statistical Weight of a DNA Match in Cold-Hit Cases*, FORENSIC SCI. COMM. (July 2009), *archived at* <https://perma.cc/5TWX-TFRZ> (describing a cold-hit case occurring when a DNA match of evidence is obtained and queried through a DNA database). In contrast with a probable-cause case, which starts with non-DNA evidence and may be bolstered by such evidence, a cold-hit case starts with DNA and then is corroborated by non-DNA facts subsequently obtained. *Id.* See generally Dennis, *supra* note 27 (noting that Virginia became the first state to execute a criminal who was serving time for a rape and scheduled to be released in 2004 but then convicted of murder and rape based on a “cold-hit” in 2002).

³⁹ See Dennis, *supra* note 27 (noting that the first “John Doe” warrant was obtained in Wisconsin in 1999). “The primary purpose of these warrants is to toll the statute of limitations in cases of violent crimes.” *Id.* See Graddy, *supra* note 5, at 230–31 (explaining that proponents argue that these types of state laws protect rape survivors’ interests and the accuracy of DNA outweighs a defendant’s right to exculpatory evidence, while opponents argue that these laws violate the exact thing that statutes of limitations are supposed to protect, namely “stale charges”).

⁴⁰ See Heidi M. Hsia & Donna Hamparian, *Disproportionate Minority Confinement: 1997 Update*, JUV. JUST. BULL. (Sept. 1998), *archived at* <https://perma.cc/JQ79-5V3F> (highlighting the racial disparity of the juvenile population that is held in correctional institutes, which has led to the term “minority overrepresentation”).

percent chance of being incarcerated at any point in his lifetime.⁴¹ The incarceration rate ties to the number of DNA samples that national or statewide databases have on file, thus skewing any database result toward minority groups.⁴² Consequently, while DNA has revolutionized criminal investigations, it spotlights one of the more troubling issues in America's criminal justice system.⁴³

B. Origin of Genealogy Databases and How They Came Online

Genealogy has quickly become a popular hobby in the United States.⁴⁴ The obsession has an interesting, albeit somewhat ignominious, history shrouded in what some may consider elitism

⁴¹ See Jan M. Chaiken, *Crunching Numbers: Crime and Incarceration at the End of the Millennium*, NAT'L INST. OF JUST. (Jan. 2000), archived at <https://perma.cc/38FT-F7EC> (noting the racial disparity skewed towards black men who are under correctional supervision).

We find that 8.3 percent of black men ages 25 to 29 were in prison at the end of 1996. This figure is more than three times higher than the 2.6 percent of Hispanic men who are in prison and more than 10 times higher than the rate for white men.

Id.

⁴² See David H. Kaye, *Two Fallacies About DNA Data Banks for Law Enforcement*, 67 BROOK L. REV 179, 199 (2001) (underscoring the fact that databases confined to convicted felons, or other people who would have their DNA collected as part of routine booking, will be disproportionately dominated by minority groups).

⁴³ See *id.* (implying that "offender-only" databases, such as CODIS, are implicitly racially disparate).

⁴⁴ See Rebecca Gold, *From Swabs to Handcuffs: How Commercial DNA Services Can Expose You to Criminal Charges*, 55 CAL. W. L. REV. 491, 493–94 (2019) (stating that there are over twelve million people who have used one or more of the 39 and counting direct-to-consumer (DTC) genetic testing companies); Antonio Regalado, *More than 26 million people have taken an at-home ancestry test*, MIT TECH. REV. (Feb. 11, 2019), archived at <https://perma.cc/6ZHW-7RD3> (emphasizing that DTC providers could hold the data of more than 26 million people within the next two years); Gregory Rodriguez, *How Genealogy Became Almost as Popular as Porn*, TIME (May 30, 2014), archived at <https://perma.cc/9347-8LPE> (noting that genealogy is the second most visited category of websites on the internet, after pornography, and it has become a billion-dollar industry).

and religious fixation.⁴⁵ Beginning in the 1960s, the Mormon Church opened genealogical libraries throughout the United States and the next decade saw more non-Mormon's coming to the libraries to research ancestral trees.⁴⁶ The proliferation of the internet in the 1990s allowed genealogical databases, which stored large amounts of information, to be digitized and allowed genealogical hobbyists to conduct research from the comfort of their own homes.⁴⁷

The big genealogy companies such as 23andMe.com and Ancestry.com used to market the at-home DNA testing kits as ways to test for diseases and understand your body.⁴⁸ Now, the pitch is to connect people to lost relatives or research one's heritage.⁴⁹ All somebody has to do is spit into a tube, and a couple months later he can log on to his account to access a wide array of fascinating

⁴⁵ See Rodriguez, *supra* note 44 (indicating that white elites wanted to maintain their social status through genealogical research to exclude European immigrants in the late 19th and early 20th centuries). Societies such as the Daughters of the American Revolution also have claimed social elitism through hereditary study to prove their descendants were the original settlers of the United States. *Id.* See also *Genealogy and the Mormon Archives*, PBS (Apr. 30, 2007), archived at <https://perma.cc/748E-VVQF> (explaining that one of the tenets of the Mormon faith is that “the dead can be baptized into the faith after their passing,” which meant that Mormon's painstakingly trade their ancestry to find those relatives who died so they may be baptized in the faith). The original records, about 2.4 million rolls of microfilm containing 2 billion traced names are locked away in a vault, but copies are readily accessible to the public at a library in Salt Lake City. *Id.*

⁴⁶ See Rodriguez, *supra* note 44 (stating the notion of the “quest for self-knowledge” through genealogical research was made easier by religion and technology).

⁴⁷ See Rafi Letzter, *How Do DNA Ancestry Tests Really Work?*, LIVE SCI. (June 4, 2018), archived at <https://perma.cc/YW8V-TFJE> (opining that genetic tests used to be theories of science fiction, but are now “a nice gift to buy your genealogy-minded aunt for her birthday); Eric Levenson, *It started as a hobby. Now they're using DNA to help cops crack cold cases*, CNN (Mar. 27, 2019), archived at <https://perma.cc/7SYU-9YTY> (stating that once the methodology of using DTC sites to solve cold cases became possible, the “floodgates opened”).

⁴⁸ See Letzter, *supra* note 47 (indicating that DTCs had to cease marketing their services as health services due to federal regulation).

⁴⁹ See Neal Ungerleider, *Ancestors, Inc.: Inside the Remarkable Rise Of The Genealogy Industry*, FAST COMPANY (July 15, 2015), archived at <https://perma.cc/D2JZ-V8BW> (quoting a writer and journalist, AJ Jacobs, “Websites have turbocharged interest in genealogy. There are plenty of people who got hooked by the websites, and want to go deeper. . .”); Letzter, *supra* note 47 (noting that DTCs market themselves as “ancestry” services, which help people connect to lost relatives and determine what part of the world one's ancestors came from).

information.⁵⁰ The exact algorithms that the companies use are undisclosed, but the concept is fairly straight forward: if the algorithm finds that a certain number of people are from a specific area and researchers know that all those people trace their heritage to that area, the website will label that group accordingly.⁵¹ The issue with the genealogy companies is that the accuracy and precision of their methodologies and algorithms are directly related to their DNA sample sizes from any specific region.⁵²

Direct-To-Consumer (“DTC”) Genealogy websites are not only tools for those curious about their ancestry, but are also utilized by law enforcement to catch criminals.⁵³ The “Golden State Killer” case brought this notion to the national forefront when California investigators arrested Joseph James DeAngelo on April 24, 2018 and later revealed they had used a genealogy website called “GEDmatch.com” to generate a list of people that eventually lead them to DeAngelo.⁵⁴ While the website did see an initial downtick of

⁵⁰ See Letzter, *supra* note 47 (explaining the process of using at-home kits and how to obtain information from the websites).

⁵¹ See *id.* (detailing how the genetic tests track ancestry against massive online libraries: through the Y chromosome, which fathers pass to their male children; the mitochondrial DNA, which mothers pass to all their children; or through the 22 non-sex chromosomes, which gives the most detailed ancestry information).

⁵² See *id.* (stating that the major companies can provide extremely detailed information on European populations because that is where the biggest samples of submitted DNA are derived, compared to the least-sampled population, Native Americans).

⁵³ See Megan Cassidy, *How forensic genealogy led to an arrest in the Phoenix ‘Canal Killer’ case*, AZ CENTRAL (Nov. 30, 2016), archived at <https://perma.cc/C7UC-DRYY> (detailing how a genealogist was able to use a publicly available DNA database to match DNA found at a crime scene from the 1990s to catch the criminal responsible for the murders of two women); Natalie Ram et al., *Genealogy databases and the future of criminal investigation*, 360 SCI. MAG., no. 6393, June 8, 2018, [hereinafter *Genealogy databases and the future of criminal investigation*], at 1078 (underscoring the idea that allowing police to conduct similar database searches is likely to lead to more solved crimes); see also *Ancestry Guide for Law Enforcement*, ANCESTRY (Feb. 1, 2020), archived at <https://perma.cc/P78M-BDWR> (creating guidelines for law enforcement); *23andMe guide for Law Enforcement*, 23ANDME (Feb. 1, 2020), archived at <https://perma.cc/MXW4-S9JW> (setting guidelines for law enforcement authorities and government agencies who are seeking user information).

⁵⁴ See Gold, *supra* note 44, at 498–99 (stating that there was finally a break in the Golden State Killer case because of GEDmatch.com); Megan Molteni, *The Key to*

users in the weeks following the Golden State Killer news, this was almost immediately counterbalanced by a drastic increase in uploads and emails from users stating how they want to donate their DNA to help catch criminals.⁵⁵

III. Facts

A. *Congressional and Judicial Attempts to Prevent an Orwellian Nightmare*

Consumer DNA websites allow law enforcement to broaden the scope of existing databases such as CODIS, revitalizing Fourth Amendment privacy concerns and provoking fear that America is turning into an Orwellian police state.⁵⁶ Setting aside constitutional concerns for now, there are two prominent federal laws that provide a federal shield against law enforcement's use of genetic databases: The Genetic Information Nondiscrimination Act of 2008 ("GINA") and Health Insurance Portability and Accountability Act of 1996 ("HIPAA").⁵⁷ GINA was designed by Congress in the wake of

Cracking Cold Cases Might Be Genealogy Sites, WIRED (June 1, 2018) [hereinafter *The Key to Cracking Cold Cases*], archived at <https://perma.cc/6HY8-GCFE> (explaining how investigators, with the help of genealogists, used GEDmatch.com, which is an "open source platform" to match DNA collected at crime scenes from the 1960s to match a familial DNA of the killer).

⁵⁵ See *The Key to Cracking Cold Cases*, *supra* note 54 (comparing how different websites are reacting to law enforcement using their services to track criminals and highlighting how the public responded positively following the Golden State Killer case).

⁵⁶ See *United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011) (holding that a state statute that permits suspicionless collection of DNA samples from arrestees did not violate the Fourth Amendment); Claire Abrahamson, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 *FORDHAM L. REV.* 2539, 2567–68 (stating that the Supreme Court has held that DNA samples collected by law enforcement are not inherently entitled to Fourth Amendment privileges because the genetic material obtained by the sites contain information for identification purposes only). See also Charlotte Ahlin, *The Meaning of 'Orwellian' Is More Complicated Than You Think – And It's Extremely Relevant To Modern Politics*, BUSTLE (May 24, 2018), archived at <https://perma.cc/5ACY-65YS> (describing the dystopian society created by George Orwell's book "1984," which paints a picture of what happens when a totalitarian government limits personal freedom through constant surveillance and "Thought Police").

⁵⁷ See *Genealogy databases and the future of criminal investigation*, *supra* note 53 (giving a brief overview of GINA and HIPAA).

public unease over privacy concerns regarding genetic data.⁵⁸ The intent of the legislation was to protect private individuals from employers and health insurance companies discriminating based on genetic information.⁵⁹ The express purpose is to “protect the public from discrimination and allay their concerns about the potential for discrimination, thereby allowing individuals to take advantage of genetic testing, technologies, research, and new therapies.”⁶⁰ GINA clarifies that “genetic information” is “health information” under HIPAA, which not only covers an individual’s personal genetic tests, but also the tests of any genetic relatives.⁶¹ Additionally, the Federal DNA Act establishes standards on testing and what may be done with the genetic information once it is uploaded into CODIS.⁶² To further

⁵⁸ Genetic Information Nondiscrimination Act of 2008, H.R. 493, 110th Cong. (enacted) (detailing the findings of Congress regarding the current patchwork of state and federal laws and the need to protect the private individual from institutional infringement on private, genetic information).

⁵⁹ See Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 894 (2015) [hereinafter *DNA by the Entirety*] (highlighting the reasons Congress acted); Jessica L. Roberts, *The Genetic Information Nondiscrimination Act as an Antidiscrimination Law*, 86 NOTRE DAME L. REV. 597, 603–04 (2011) (explaining that more than ninety percent of polled Americans feared their genetic information would be misused by employers to discriminate against them based on a heightened proclivity to certain diseases, or by health insurers who would deny coverage or raise premiums based on potential genetic risk factors). See also 42 U.S.C. § 2000ff–1 (2008) (codifying how employers may not discriminate against private individuals based on genetic information).

⁶⁰ See H.R. 493 (stating the purpose of the legislation); see *DNA by the Entirety*, *supra* note 59, at 894–95 (quoting language from GINA).

⁶¹ 29 U.S.C. § 1191(b) (defining genetic information); see Roberts, *supra* note 59, at 621 (furthering the point that GINA protects the individual’s test and tests of family members of that individual as well as what a test entails); see also *DNA by the Entirety*, *supra* note 59, at 894–95 (discussing how Congress tied genetic information to health information through HIPAA). HIPAA protects an individual from discrimination based on identifiable information, and there is debate as to whether genetic information is truly identifiable or not. *Id.* at 894. See also 45 C.F.R. § 164.502(d)(2) (2014) (specifying regulations as to what information is protected against a covered entity); *DNA by the Entirety*, *supra*, at 895 (raising concerns over whether genetic information can be considered identifiable).

⁶² See Derek Regensburger, *DNA Databases and the Fourth Amendment: The Time Has Come to Reexamine the Special Needs Exception to the Warrant Requirement and the Primary Purpose Test*, 19 ALB. L.J. SCI. & TECH. 319, 329–30 (2009) (noting that the Federal DNA Act prescribes that: DNA uploaded into CODIS must come from accredited labs that meet or exceed quality standards established by the

establish a buffer against privacy violations, states have enacted statutes to protect individuals from institutions seeking to use genetic information against them.⁶³ Furthermore, federal statutes acknowledge the privacy implications of collecting and storing DNA samples and have codified the necessary steps to protect the privacy of individuals, while simultaneously prescribing penalties for abuse.⁶⁴

B. Breaking of the Dam: How Genetic Information is Legally Obtained by Law Enforcement

Enacted federal laws, such as GINA, protect against disclosure of genetic test results, but the nexus of genetic privacy

FBI; strict requirements for use; samples may only be disclosed to criminal justice agencies for identification purposes; and expungement of records where cases have been overturned).

⁶³ See ALASKA STAT. ANN. § 18.13.010 (b) (West 2019) (protecting privacy of DNA samples and results of DNA analysis except for samples collected and analyzed for law enforcement purposes, paternity testing, newborn screening, and emergency medical treatment); ARIZ. REV. STAT. ANN. § 12-2802 (A) (West 2019) (stating that information derived from genetic testing may only be released to person tested or others with written authorization and places restrictions on disclosing or compelling information of a minor without consent of a parent or guardian); COLO. REV. STAT. ANN. § 10-3-1104.6 (West 2019) (setting forth that genetic information is the property of an individual and written consent is required for disclosure, provides exceptions, and imposes penalties and grants remedies to those individuals whose rights are violated); GA. CODE ANN. § 33-54-1 (West 2019) (furthering that genetic information is the property of the individual and any health care corporation or health insurance plan outside of ERISA's jurisdiction may not seek information derived from genetic testing, and if it is received, may not be used for any nontherapeutic purpose or be released without written consent); 410 ILL. COMP. STAT. ANN. 513/15 (West 2009) (stating that genetic testing and information derived from the test may be released only to the individual and authorized persons, except if a biological sample is legally obtained by law enforcement and may only be disclosed for purposes of criminal investigations); KY. REV. STAT. ANN. § 304.12-085 (West 2019) (insurers may not discriminate against any participant or beneficiary based on genetic testing or disclose any genetic test without prior authorization); MD. CODE ANN., STATE GOV'T § 20-601 (West 2019) (stating that an employer may not discriminate against an individual because of genetic information or refusal to divulge genetic information, or request a genetic test conditioned on hiring or determining benefits).

⁶⁴ See 34 U.S.C. § 12592 (dictating what the FBI may and may not do with the index of DNA records as well prescribed penalties if procedures are violated); 34 U.S.C.A § 40706 (enunciating privacy protection standards); 34 U.S.C. § 12593 (detailing proficiency testing standards for personnel and laboratories associated with collecting and storing DNA).

debates center around DNA collection, databases, and the Fourth Amendment.⁶⁵ Supreme Court cases such as *Katz v. United States* or *United States v. Jones* are the jurisprudential touchstones pertaining to illegal search and seizures under the Fourth Amendment.⁶⁶ However, the Supreme Court held in *Maryland v. King* that Maryland's statute authorizing law enforcement to collect samples from arrestees is constitutional under the Fourth Amendment.⁶⁷ A primary reason that DNA collection is valid under the Fourth Amendment is that it has been analogized to collecting fingerprints from a crime scene or from an arrestee during booking procedures.⁶⁸ The Court has also articulated that unwarranted searches are permitted in some instances, such as searches justified by "special needs" and searches of people with reduced expectations of privacy.⁶⁹

⁶⁵ See *DNA by the Entirety*, *supra* note 59, at 897 (asserting that there is a "[C]onstitutionally relevant interest in identifiable, medically relevant genetic information.").

⁶⁶ See *U.S. v. Jones*, 565 U.S. 400, 410 (2012) (holding that the defendant's Fourth Amendment rights were violated because FBI agents did not have a valid warrant by the time the GPS tracker was attached to the vehicle); *Katz v. U.S.*, 389 U.S. 347, 351, 353 (1967) (holding that the Fourth Amendment protects "people, not places", and therefore, when a person seeks to keep something private, even in a public area, that *may* be constitutionally protected under the Fourth Amendment) (emphasis added).

⁶⁷ See *Maryland v. King*, 569 U.S. 435, 465–66 (2013) (deciding that the fact that taking an arrestee's DNA is akin to routine booking procedures such as fingerprinting and photographing, which does not violate an arrestee's diminished expectation of privacy; and the brief swab of an arrestee's cheek does not constitute such an invasion or intrusion that it would violate the Fourth Amendment).

⁶⁸ See *United States v. Mitchell*, 652 F.3d 387, 413 (3rd Cir. 2011) (stating that DNA profiling is a more precise method of identification and is akin to fingerprinting). See also *Anderson v. Commonwealth*, 650 S.E.2d 702, 705 (Va. 2007) (analogizing DNA taken from an arrestee to fingerprinting, while admitting that DNA samples are more revealing). The reason that courts have been able to take this stance is that the DNA used in analysis for identification purposes is "non-coding", and thus do not reveal any personal traits or private information. *Id.* See Gabel, *supra* note 33, at 578 (noting that courts have embraced the analogy between fingerprinting and DNA analysis).

⁶⁹ See *N.J. v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (clarifying an exception to the warrant and probable-cause requirement where "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable"); *Nicholas v. Goord*, 430 F.3d 652,

Further, the Court has relied upon the “third-party” doctrine, which essentially states that once a person voluntarily gives up his information to a third-party, he has no legitimate expectation of privacy.⁷⁰ The scope of the third-party doctrine has extended to bank records, telephone records, and IP addresses.⁷¹ However, a person does not completely abandon his rights when giving information to a third party.⁷² This sentiment is furthered in *Carpenter v. U.S.*, which some believe has watered-down the scope of the third-party doctrine.⁷³ While this seems like a victory against governmental over-reach into personal lives, the ruling is a narrow one which declined to extend the third-party doctrine to information gleaned from cell phones that reveal an “intimate window into a person’s life”.⁷⁴

666–67 (2d Cir. 2005) (asserting that almost every special-needs case involves an individual with a diminished right of privacy); *see also* Regensburger, *supra* note 62, at 343 (delineating the five categories of permissible searches that do not require reasonable suspicion).

⁷⁰ *See* *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (holding that the defendant did not have a reasonable expectation of privacy when he turned his information over to a third party).

This Court has repeatedly held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

See *U.S. v. Miller*, 425 U.S. 435, 443 (1976).

⁷¹ *See* *Abrahamson*, *supra* note 56, at 2556 (explaining that this information is not protected by the Fourth Amendment through the third-party doctrine and may be legally obtained by law enforcement without a warrant).

⁷² *See* *Carpenter v. U.S.*, 138 S.Ct. 2206, 2217 (2018) (“what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”) (quoting *Katz v. United States*, 389 U.S. 347, 351–52 (1967)).

⁷³ *See id.* at 2220 (holding that the government may generally need a warrant to collect historical cell-site location information from an individual’s cell-phone, but left the door open to exceptions such as exigent circumstances or emergency situations); *see also* Paul Ohm, *The Broad Reach of Carpenter v. United States*, JUST. SEC. (June 27, 2018), *archived at* <https://perma.cc/U7KU-5NJ7> (declaring the third-party doctrine is “almost dead” and lays out the case that defendants will test the boundaries of the case to expand the holding to other kinds of information collected by law enforcement).

⁷⁴ *See* *Carpenter*, 138 S.Ct. at 2217 (noting that cell phones are so pervasive and necessary for modern life and the information they reveal through cell-site records are deeply personal and should be protected).

C. *A Weighted Interest: The Significance of DNA in Law Enforcement and how DTC Genealogy Websites Have Helped*

The courts have grappled with Fourth Amendment violations by balancing the subjective privacy expectations of an individual against reasonable expectations of society and the government's interest.⁷⁵ As with DNA and its use in criminal investigations, the governmental interest in correctly identifying suspects is substantial.⁷⁶ As previously stated, the Golden State Killer case is compellingly the most notable cold case solved by matching forensically archived DNA against DTC sites, but there are many other success stories.⁷⁷

⁷⁵ See Abrahamson, *supra* note 56, at 2555–56 (highlighting what the traditional approach is as exemplified in the *Katz* case).

⁷⁶ See *U.S. v. Sczubelek*, 402 F.3d 175, 186 (3d Cir. 2005) (describing how the government's primary goals of rehabilitation and deterrence are served by collecting identifying information); B.E. Witkin et al., *California Criminal Law § 60 Constitutionality*, 4 WITKIN CAL. CRIM. LAW 4TH CRIM. PROC. (2019) [hereinafter Witkin] (enunciating the fact that the government has a substantial interest in accurately identifying criminals because DNA is uniquely effective and the intrusion of collection is minimal). See also 22 Cal. Jur. 3d Criminal Law: Posttrial Proceedings § 41 (2019) (stating that the government has a compelling interest in collection of DNA samples, through reasonable force, as it serves as a deterrent in preventing future criminality); Kaye, *supra* note 42, at 180 (commenting on the fact that law enforcement discovered that recidivism rates for felonies are comparable to most sex crimes, incentivizing creation and use of DNA databases); see generally David Canter & Donna Youngs, *Crime and Society*, TAYLOR & FRANCIS ONLINE (Dec. 1, 2016), archived at <https://perma.cc/ECY2-W9WF> (outlining the destructive force of criminality on society); but see Andrea Roth, “*Spit and Acquit*”: Prosecutors as Surveillance Entrepreneurs, 107 CALIF. L. REV. 405, 412–13 (Apr. 2019) (citing a study that questions DNA databases deterrence value and power to exonerate based on the fact that it may only be persons convicted of “serious” crimes that may be deterred by such databases because there is little evidence to support that expanding databases will lower crime rates among misdemeanants) (emphasis added).

⁷⁷ See Patrick May, *Chilling tales from the Golden State Killer’s rampage*, THE MERCURY NEWS (Apr. 28, 2018), archived at <https://perma.cc/KC8R-8X2S> (detailing the charges that were filed to date after the suspect was caught); Faith Karimi, *A girl was found dead at the beach after a bike ride in 1972. DNA helped police identify a suspect*, CNN (Sept. 12, 2019), archived at <https://perma.cc/WU4Z-GYQN> (detailing how police were able to convict a man who raped and killed an eleven-year-old girl through DNA evidence left at the scene linked to DNA submitted to a genealogical database by a relative); Levenson,

Genealogists have conducted independent research on the accuracy of DTC sites in narrowing down a field of suspects through the use of a hypothetical DNA dataset in a test case—they were able to narrow down a list of 850 suspects to 17.⁷⁸ While the advantages are self-evident in assisting law enforcement to solve cold cases, there are concerns over the terms and conditions accompanied by these various sites.⁷⁹ There is a legislative and constitutional basis for allowing law

supra note 77 (highlighting cold cases that were solved uses DTC genealogy websites). It is also important to note that cross-referencing DNA collected at crime scene to a DTC site or government database, such as CODIS, is the first step in a long investigatory process. *Id.* Glen Martin, *Gird Your Genes: What DNA Matching Might Mean for Your Privacy*, CALIFORNIA MAG. (July 2018), archived at <https://perma.cc/WP86-N5TQ> (explaining implications of capturing The Golden State Killer).

⁷⁸ See Jocelyn Kaiser, *We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans*, SCIENCEMAG (Oct. 11, 2018), archived at <https://perma.cc/P64R-PN8S> (explaining how small of a genealogical database could be in order to conduct an investigation based on DNA); Megan Molteni, *What the Golden State Killer Tells Us About Forensic Genetics*, WIRED (Apr. 24, 2019) [hereinafter *What the Golden State Killer Tells Us About Forensic Genetics*], archived at <https://perma.cc/E87C-6FTG> (detailing how genealogical research through DTC databases has been used to identify more than fifty suspects in criminal investigations with the potential to solve thousands more); see also Damian Garde, *'What's my real identity?': As DNA ancestry sites gather more data, the answer for consumers often changes*, STATNEWS (May 22, 2019), archived at <https://perma.cc/EB7H-2Y6F> (noting that the two biggest DTC companies, 23andMe and Ancestry, both claim to have tested more than 25 million people to date).

⁷⁹ See Abrahamson, *supra* note 56, at 2554 (admitting DTC provides a valuable resource because where there have been no leads in cold cases they are able to generate a small suspect pool); *Ancestry 2020 Transparency Report*, ANCESTRY (Feb. 1, 2020), archived at <https://perma.cc/3CM7-GTZM> (discussing Ancestry's commitment to protecting customers' data by providing transparency about when they receive requests for law enforcement access to it); *The Coalition for Genetic Data Protection*, GENETIC DATA PROT. (Feb. 1, 2020), archived at <https://perma.cc/4NVY-KZRD> (detailing Ancestry and 23andMe transparency reports, policies and procedures, disclosure statements, and rules for law enforcement). See also Kristen V. Brown, *What DNA Testing Companies' Terrifying Privacy Policies Actually Mean*, GIZMODO (Oct. 18, 2017), archived at <https://perma.cc/2B4F-6SGA> (stating that informed consent only shows up once when registering for a DNA kit); Edward C. Baig, *DNA testing can share all your family secrets. Are you ready for that?*, USA TODAY (July 9, 2019), archived at <https://perma.cc/WZF4-W4NC> (revealing 40% of DTC companies had no policy available to consumers on their website or had policies that did not mention genetic data). Companies that did have a visible policy often included vague boilerplate language. *Id.* But see Abrahamson, *supra* note 56, at 2565 (stating that

enforcement to use DTC websites to supplement their investigations, but contention exists in defining the legal parameters of this practice.

IV. Analysis

A. *When the Horse Saw the First Car*

It is still debated whether Henry Ford actually said, “[i]f I had asked people what they wanted, they would have said faster horses,” however the idea of breaking away from an existing paradigm to innovate and create change continues to resonate. When examining the law and criminal investigations, this sentiment of how change should be embraced continues to apply as new technology emerges.⁸⁰ Accepting change is the starting point; however, the complex issue of using DTC databases to match DNA found at a crime scene opens a proverbial Pandora’s box of individualistic threats.⁸¹ These threats may be invasion of privacy, encroachment on personal identity, or a desire to remain anonymous in an increasingly connected world.⁸² There is also the fear of inaccurate results that invariably may happen in any criminal investigation caused by factors such as contamination, interpretive error, or plain coincidence.⁸³ These concerns cannot be hand-waived as improbabilities brought about by fear of change because they deal with notions of American liberty; but at the very least they can be assuaged by the science behind DNA

“clickwrap” terms on DTC websites are typically binding on consumers and establish an assumption of risk under the third-party doctrine).

⁸⁰ See *Serge*, 896 A.2d at 1178 (exemplifying the willingness of courts to adapt scientific progress in admitting evidence of computer-generated animation in the courtroom to show how the victim was murdered based on forensic evidence).

⁸¹ See Gold, *supra* note 44, at 497 (arguing that with the arrival of new technology individuals have a decreased sense of privacy).

⁸² See Kaye, *supra* note 42, at 192 (noting the apprehension to the mere housing of DNA in databanks “trespasses into a ‘sphere of inviolability’, disrupting ‘autonomy, dignity, and physical integrity’”); Martin, *supra* note 77 (admitting that while “familial searches” are protected by varying statutory regulations, open-source websites allow anybody “free rein to dig through your genetic data . . .”).

⁸³ See Roth, *supra* note 76, at 414–15 (stating that, although unlikely, an innocent person might be implicated in a crime because of an erroneous DNA match, cyber breaches, human error, or scene/lab contamination).

and the legal framework that defines the use of DTC, state, and federally operated DNA databases.⁸⁴

Individuals willingly divulge information through the use of credit cards, cell phones that can track every movement, and social media.⁸⁵ The law has allowed investigators to use this information to solve crimes within constitutional, statutory, and evidentiary bounds.⁸⁶ The law has also dictated how DNA is collected, stored, and used in criminal investigations, with further emphasis on restrictions regarding the use of DNA outside the criminal sphere.⁸⁷ As individuals continue to use DTC websites, and thus continue to submit DNA for analysis, the question of whether relatives of DTC customers have a right of privacy becomes even more pertinent.⁸⁸

⁸⁴ See 34 U.S.C.A. § 12592 (dictating what the FBI may and may not do with the index of DNA records as well proscribed penalties if procedures are violated); 34 U.S.C.A. § 40706 (enunciating privacy protection standards); *supra* text accompanying note 58; *Mitchell*, 652 F.3d at 413 (highlighting the fact that DNA profiling is more accurate than fingerprint analysis); Roberts, *supra* note 59, at 625 (describing GINA as a forward-thinking statute designed to protect against discrimination, which is compared to other anti-discrimination statutes that were reactive pieces of legislation). See also Gabel, *supra* note 33, at 578 (admitting that stored in federal or state databases do not reveal any information beyond identity because the DNA segments are “non-coding”).

⁸⁵ See Gold, *supra* note 44, at 497 (noting that privacy has been a concern with the advent of the modern age, and particularly social media). “Social media, text messaging, online shopping, and other services allow the average American to share a significant amount of information with each other daily.” *Id.* (emphasis added).

⁸⁶ See Gold, *supra* note 44, at 497 (stating that the third-party doctrine allows the government to access cell phone records and social media that circumvents normal Fourth Amendment protections).

⁸⁷ See 34 U.S.C.A. § 12592 (dictating what the FBI may and may not do with the index of DNA records as well as enumerating penalties if procedures are violated); 34 U.S.C.A. § 40706 (enunciating privacy protection standards); 34 U.S.C.A. § 12593 (detailing proficiency testing standards for personnel and laboratories associated with collecting the storing DNA).

⁸⁸ See Gold, *supra* note 44, at 493 (arguing that since over 12 million people have used a DTC company to test their genetic code, there are legitimate civil and criminal privacy concerns); Gabel, *supra* note 33, at 579 (questioning the assertion that the “non-coding” segments of DNA stored in databases do not reveal more than identity and points to the fact that scientific and medical advancements may be able to reveal personal characteristics); Abrahamson, *supra* note 5656, at 2551 (stating that DTC providers are not subject to the same federal and state regulation as CODIS). There are issues of ownership rights stemming from DTC providers own user agreements, such as 23andme.com, which states that users “assign a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to

Given the social interest in solving crimes, law enforcement should be allowed to use DTC genealogy services to compare DNA evidence in criminal investigations within the current legal framework currently applied to existing state and federal databases.⁸⁹

B. *Hiding in Plain Sight*

The most functional way to analyze the use of DTC DNA repositories in criminal investigations is to talk about a concrete example of their functionality in solving crimes.⁹⁰ Discussing this complex issue in the abstract takes away from not only the probative value that this use of technology has in a courtroom, but also the societal demand for justice that it satisfies.⁹¹ As previously discussed, the Golden State Killer case is one of the most popular illustrations of how investigators used this new method to solve a fifty-year-old cold case.⁹² The terroristic grip that Joseph DeAngelo had on California and the nation in the mid-1970's through mid-

reproduce, adapt, modify, translate, publish, publicly perform, publicly display, distribute, reproduce, edit, reformat, and create derivative works from any [submitted] User Content.” *Id.* at 2552.

⁸⁹ See Graddy, *supra* note 5, at 227 (arguing that DNA evidence is superior than most other forms of evidence because of its reliability, accuracy, longevity, and deterrence factor).

⁹⁰ See *What the Golden State Killer Tells Us About Forensic Genetics*, *supra* note 78 (stating that “investigative genetic genealogy has emerged as the most powerful crime-fighting tool since DNA itself.”).

⁹¹ See Regensburger, *supra* note 62, at 336–37 (citing a case that highlighted the fact that the most probative evidence relating to DNA is whether or not the evidence matches the suspect); see also Graddy, *supra* note 5, at 227–28 (commenting that states impose different thresholds regarding the collection of DNA ranging from some classes of misdemeanors to only those convicted of homicide and sexual assault). See Kaye, *supra* note 42, at 190–91 (advocating for more comprehensive DNA databases). There is no identifiable harm including more crimes as qualifying as offenses in DNA databases. *Id.* at 191–92.

⁹² See Regalado, *supra* note 44 (observing that the public was not aware of the applicable effects of DTC databases until the Golden State Killer was caught and since that point, more than thirty rapists, killers, and victims’ bodies have been identified using the same method); Gold, *supra* note 44, at 499 (noting that the Golden State Killer case has inspired others to use DTC provider databases to search for other notorious criminals such as the Zodiac Killer).

1980's cannot be understated.⁹³ The case shed a light on some of our greatest fears: invasion of one's home, psychological torture, rape, murder, and the helplessness stemming from the inability to apprehend the person behind these monstrous acts.⁹⁴

DeAngelo's infamous crimes were aided by his ability to hide in plain sight, as a police officer; using fear as his weapon and anonymity as his shield.⁹⁵ A perceived right to anonymity is not the same as a right of privacy, which includes extensive protection from government intrusion into one's home afforded by Fourth Amendment jurisprudence.⁹⁶ These two concepts, anonymity and privacy, seem to get conflated.⁹⁷ As people necessarily become more reliant on technology to store and manage personal information, it makes sense that individuals would want their data to be protected in the modern age.⁹⁸ This is not to say that the desire to be anonymous is not unwarranted in some situations.⁹⁹ However, it does carry a

⁹³ See *What the Golden State Killer Tells Us About Forensic Genetics*, *supra* note 78 (articulating how he had "spread terror" throughout the state for more than forty years).

⁹⁴ See *May*, *supra* note 77 (detailing DeAngelo's crimes).

⁹⁵ See *Gold*, *supra* note 44, at 498 (noting that DeAngelo was not caught for over forty years and it turned into a cold case); see also *Mitchell*, 652 F.3d at 414 ("It is a well-recognized aspect of criminal conduct that the perpetrator will take unusual steps to conceal not only his conduct, but also his identity.").

⁹⁶ See *Kaye*, *supra* note 42, at 193 (arguing that privacy is not put at risk when the government can match DNA evidence with a profile found on a database). The concept of anonymity is no longer feasible in today's modern age, and it is not a Constitutional right:

[T]he interest in changing or obscuring one's identity is not a constitutionally recognized right or morally profound interest. It may be desired by many people intent on committing crimes; surely, it is a rare offender who expects to be identified and apprehended when he or she commits a crime. If no one knows who they are, these offenders may well elude apprehension; conversely, there is no special trick to apprehending a burglar, a robber, or a hit-and-run driver whose name can be given to police by a passerby. A comprehensive DNA identification data base reduces such anonymity for offenders—and for the rest of us.

Id. at 194.

⁹⁷ See *Kaye*, *supra* note 42, at 193–94 (distinguishing privacy and the "romantic, unrealistic prospect" of disguising or altering an identity, which would be of little-to-no practical importance beyond a desire to commit crimes).

⁹⁸ See *Gold*, *supra* note 44, at 492–93 (arguing that the public's expectation of privacy is objectively the same even though technology has changed, and the law should reflect that sentiment).

⁹⁹ See *Kaye*, *supra* note 42, at 193 (recognizing the American notion of re-invention).

negative connotation, which can be exemplified by the ever-present issue of cyber-bullying, catfishing, and extortion by anonymous social media accounts.¹⁰⁰ Revealing the identity of faceless predators and bringing them to justice not only incapacitates them, but hopefully serves as a deterrent for others.¹⁰¹ After forty years, investigators were able to put an actual name to the nebulous evil that was the Golden State Killer.¹⁰²

DNA evidence was not available when these crimes were committed, which included at least twelve murders, more than forty-five rapes, and over one hundred burglaries.¹⁰³ However, even if DNA analysis was able to be used in the investigations, detectives likely would not have been able to match samples found at the crime scene to any known perpetrator.¹⁰⁴ Fast forward to 2018, where investigators used an open source DTC website to match a distant relative's DNA to DeAngelo's DNA found at multiple crime scenes.¹⁰⁵

¹⁰⁰ See *Top five social media privacy concerns*, *supra* note 8 (explaining that social media presents the following risks: hacking and impersonation; stalking and harassment; phishing; and the dangers of sharing location-based data).

¹⁰¹ See Regensburger, *supra* note 62, at 372–73 (highlighting the fact that DNA evidence's capacity to identify or exclude individuals serves a deterrent effect not only for the person convicted of a crime, but for society as a whole); Kaye, *supra* note 42, at 194 (noting that the very existence a comprehensive database would "make it harder to pursue a life of crime").

¹⁰² See *What the Golden State Killer Tells Us About Forensic Genetics*, *supra* note 78 (stating that it took forty years to catch DeAngelo).

¹⁰³ See Gold, *supra* note 44, at 498 (giving a brief overview of the decade long crime spree of the Golden State Killer).

¹⁰⁴ See *Combined DNA Index System*, *supra* note 34 (noting that the FBI started the DNA index pilot program in 1990); *The science behind genetic fingerprinting*, *supra* note 21 (discussing how the first case to use DNA was in 1984); see also Regensburger, *supra* note 62, at 336–37 (determining that the highest probative value of DNA evidence is being able to compare samples found at a crime scene to an actual individual).

¹⁰⁵ See Gold, *supra* note 44, at 498–99 (explaining how investigators caught DeAngelo using GEDMatch.com); Regalado, *supra* note 44 (clarifying that GEDMatch.com is a database where people share test results from other companies).

C. *Thirteen Reasons Why*

The genetic sequence used to identify individuals does not disclose much more information than relatedness to other people.¹⁰⁶ In fact, relatedness is the mission statement of most of these websites.¹⁰⁷ Customers have discovered previously unknown ancestors, distant living relatives, and even found siblings they did not know they had.¹⁰⁸ These revelations could be exceedingly joyous or incredibly disheartening depending on the circumstances.¹⁰⁹ Unfortunately, for one individual that submitted their DNA to GEDMatch.com, their distant relative turned out to Joseph DeAngelo.¹¹⁰

The successful capture of DeAngelo does not come without criticism surrounding the methods employed by investigators, particularly due the open nature of the DTC website used, GEDMatch.com.¹¹¹ This website offers limited privacy protection to users, and the company allowed access to its database without a warrant or subpoena, as is required by the major DTC sites such as

¹⁰⁶ See Abrahamson, *supra* note 56, at 2547 (articulating that forensic DNA tests analyze thirteen “loci”, which have been referred to as “nonprotein coding junk regions of DNA”); see Letzter, *supra* note 47 (explaining how DTC algorithms work).

¹⁰⁷ See Letzter, *supra* note 47 (asserting that U.S. regulators forced DTC providers to market themselves as ancestry services, rather than health services); see also *Ancestry Guide for Law Enforcement*, *supra* note 53 (explaining their DNA testing service, which “connects autosomal test results with our DNA database to estimate a user’s ethnicity and identify relationships with unknown relatives.”).

¹⁰⁸ See Letzter, *supra* note 47 (noting that finding long lost relatives is relatively easy for DTC companies); Kaiser, *supra* note 78 (revealing that there is a 60% chance that one has a third cousin or closer in MyHeritage.com’s database if you live in the U.S. or have European ancestry).

¹⁰⁹ Compare Rodriguez, *supra* note 44 (describing the personal admiration the author felt to his father who had put together a comprehensive family history), with Martin, *supra* note 77 (addressing the hypothetical situation where a distant relative submits DNA, which indirectly implicates an innocent person because his or her “long-lost evil twin” commits a crime).

¹¹⁰ See Gold, *supra* note 44, at 499 (explaining that police matched crime scene evidence with a positive familial match on GEDMatch.com).

¹¹¹ See *id.* (describing GEDMatch.com as an “open-source” platform that warns users that their information can be “accessed for uses other than ancestry searches”); Martin, *supra* note 77 (explaining that data may be uploaded by third parties to GEDMatch.com to find more matches, and anyone may access that information).

Ancestry.com or 23andme.com.¹¹² Admittedly, this lack of checks and balances raises questions of privacy violations related to the disclosure of possibly the most intimate facet of self—our genetic code.¹¹³ While this specific instance does give pause, it needs to be understood that the genetic information (specifically the thirteen non-coding loci) analyzed by these DTC databases does not provide height, weight, hair color, location, or any other personal descriptors beyond genealogy and the previously mentioned possibility of relatedness.¹¹⁴ Meaning, investigators still need to do pain staking research to map out family trees, fetter out statistical inaccuracies, and do the ancillary legwork to determine the actual criminal.¹¹⁵

¹¹² See *Ancestry Guide for Law Enforcement*, *supra* note 53 (stating that the company will “release basic subscriber information as defined in 18 USC § 2703(c)(2) about Ancestry users to law enforcement only in response to a valid trial, grand jury, or administrative subpoena.”); *Ancestry 2018 Transparency Report*, *supra* note 79 (acknowledging that the service received nine valid law enforcement requests for user information, which contained one request seeking access to the DNA database through a search warrant that was challenged and therefore did not require the company to provide any customer data); *The Coalition for Genetic Data Protection*, *supra* note 79 (announcing that major DTC providers create and adhere to policies and procedures to protect consumer data and privacy).

¹¹³ See Gold, *supra* note 44, at 502–03 (arguing that advancements in technology creates incentives for abuse of consumer DNA databases).

¹¹⁴ See Regensburger, *supra* note 62, at 377 (stating that DNA profiles do not express any personal traits about an individual beyond a record of that person’s identity); *DNA by the Entirety*, *supra* note 59, at 880 (stating that the great majority of human DNA is noncoding, and that forensic genetic science treats the distinction between coding and noncoding seriously). Furthermore, some states explicitly prohibit forensic testing of coding DNA that could predict health. *Id.* at 880–81.

¹¹⁵ See Regensburger, *supra* note 62, at 338 (highlighting the fact that a DNA database hit is only the beginning of an investigation because it puts the person at the crime scene). DNA evidence points investigators to the person, but the investigation still needs to confirm that fact along with other elements of the crime such as motive. *Id.* See Martin, *supra* note 77 (stating that “investigations involving open source databases are unlikely to become widespread because they’re extraordinarily complex, time-consuming, and expensive”); Levenson, *supra* note 46 (noting that genealogical research does not end with DTC websites, even open-source sites like GEDMatch.com, as it still requires genealogists to comb through obituaries, birth certificates, and other public records to build a family tree).

D. Blind Justice

There is little debate that the American criminal justice system convicts and incarcerates a disproportionate number of minorities compared to the relative population.¹¹⁶ Based on estimates, 14% of black males are incarcerated before adulthood, compared with 0.8% of white males.¹¹⁷ This being the case, it may reason that state and federal established DNA databases, such as CODIS, skew heavily towards these disparate numbers.¹¹⁸ Allowing law enforcement access to DTC databases, however, may swing the pendulum to a more statistically representative number.¹¹⁹ A more comprehensive cross section of the population allows investigators to draw from a larger number of possible suspects without inviting as much conscious or unconscious racial bias.¹²⁰ The Innocence Project has cited 367 exonerations based on DNA evidence since 1989, of which 70% were classified as minorities.¹²¹ Using DTC databases would give the court more tools to exonerate and solve cold cases, importantly remedying lapses of justice.¹²²

¹¹⁶ See Kaye, *supra* note 42, at 195 (offering that adult black men are four times more likely to be under correctional supervision than white men).

¹¹⁷ See *id.* at 194–95 (demonstrating the racial disparities in the criminal justice system).

¹¹⁸ See Abrahamson, *supra* note 56, at 2547 (articulating that publicly available reports indicate that an estimated “8.6 percent of the entire African American population is currently in [CODIS], compared with only 2 percent of the white population”).

¹¹⁹ See *id.* at 2549 (noting that nearly 80% of DTC consumers tend to have European descent); *Genealogy databases and the future of criminal investigation*, *supra* note 53, at 1078 (stating that 23andMe “consists disproportionately of individuals of European descent”).

¹²⁰ See Kaye, *supra* note 42, at 196 (arguing that it is problematic to have a system that we know inherently punishes minorities disproportionately, however, more comprehensive DNA databases may alleviate some of these issues).

¹²¹ See *DNA Exonerations in the United States*, *supra* note 4 (citing statistics of exonerated individuals through the Innocence Project).

¹²² See Kaye, *supra* note 42, at 196 (arguing for the immutability and precision of DNA evidence in being able to identify a possible suspect, regardless of race); *Genealogy databases and the future of criminal investigation*, *supra* note 53 (advocating for the use of genealogical databases in law enforcement to remedy the racial disparities that occur in traditional forensic investigations).

E. Limiting the Scope

Currently, there are no governmental controls on the relationship between DTC providers and law enforcement.¹²³ The only restrictions that govern these websites are self-imposed.¹²⁴ While there are benefits to allowing law enforcement access to these resources, there also needs to be limitations to alleviate privacy concerns surrounding their use.¹²⁵ Existing legislation such as GINA and HIPAA protect against disclosure of private health information to entities such as insurance companies.¹²⁶ However, there are no analogous restrictions to government actors, as evidenced by the DNA Act.¹²⁷ A start in the right direction would be to require that genetic code obtained through DTC sites and used in criminal investigation should be limited to non-coding sections, akin to what is stored in CODIS.¹²⁸ The most logical solution would be to regulate governmental use of DTC providers using the same legal framework surrounding the use of CODIS and state-run criminal DNA

¹²³ See Abrahamson, *supra* note 56, at 2568 (acknowledging that there are no statutes regulating investigatory usage of DTC services).

¹²⁴ See Gold, *supra* note 44, at 502 (addressing the fact that DTC databases are not governmentally regulated). While Ancestry.com states that it will not disclose user information without a proper warrant, this may be just a contractual nicety to put users at ease because police may circumvent the warrant requirement through the use of the third-party doctrine. *Id.* at 503.

¹²⁵ See *DNA by the Entirety*, *supra* note 59, at 899 (analyzing the current legal framework as inadequate to adjudicate ownership and control of genetic information because it is shared among the population, giving rise to privacy concerns).

¹²⁶ See *id.* at 894–95 (detailing the legislative protections that encompass privacy protections and the intent behind the measures). Importantly, GINA defines “‘genetic information’ to include not only an individual’s own genetic tests, but also the tests of genetic relatives.” *Id.* at 895.

¹²⁷ See Abrahamson, *supra* note 56, at 2585 (noting the lack of regulatory or legislative oversight). No legislators, besides Senator Chuck Schumer, have called for oversight from the Federal Trade Commission (FTC) or expansion of definitions under HIPAA to include DTC consumers. *Id.* at 2583–84.

¹²⁸ See Kaye, *supra* note 42, at 187 (asserting that limiting the government to non-coding loci is appropriate to avoid revealing personal features of an individual, which would thus limit privacy concerns).

databases.¹²⁹ As a result, a balance may be struck between the weighty interest of government and society in accurately identifying suspects against the public's subjective and objective expectations of privacy.

V. Conclusion

Criminal investigations and forensic science have gone through iterative changes throughout history. Methodology and crime scene analysis has largely coincided with technological evolution, and the law has often been slow to catch up, especially in the modern age as developments occur more rapidly and often without notice. The law's deliberate and slow progress towards the curve of change is foundational to making sure, as a society, there are defenses against abuse of power and individuals are protected against governmental overreach. While personal freedoms are a cornerstone of America's Constitutional ideology; societal and governmental interests in apprehending the true criminal also must be weighed.

Arguably, the most powerful tool in identification in criminal cases is DNA evidence. Using all possible resources at their disposal, law enforcement should be able to use DTC website databases to match DNA evidence found at crime scenes with potential suspects. This does not mean that investigators have a free pass to sift through a user's human genome. There are statutory regulations, as well as common law backstops, that provide a framework to guide legislators and the courts. Allowing law enforcement at the state and federal level to use DTC websites does not replace or upend the investigative process, but instead gives those charged with catching a criminal the resources to do it correctly.

¹²⁹ See *id.* at 188 (noting that CODIS uses exclusively non-coding parts of the genome, which do not correspond with "observable traits."); see also Witkin, *supra* note 76 (noting that society and the government has a vested interest in apprehending the *correct* suspect) (emphasis added).