

*MARYLAND V. KING* AND THE ROAD ALREADY TRAVELED:  
 HOW THE UNITED KINGDOM TRIED—AND FAILED—TO  
 BALANCE STATE INTERESTS WITH PRIVACY RIGHTS

Courtney A. Coons Poole\*

TABLE OF CONTENTS

I.	INTRODUCTION .....	158
	<i>A. Background on Forensic DNA Analysis</i> .....	162
II.	THE U.K. LEGISLATION .....	164
	<i>A. The Royal Commission on Criminal Justice’s 1993</i> <i>Recommendation</i> .....	165
	<i>B. The Criminal Justice and Public Order Act</i> .....	166
	<i>C. The Criminal Evidence (Amendment) Act</i> .....	167
	<i>D. The Data Protection Act of 1998</i> .....	168
	<i>E. The Police and Criminal Evidence Act of 1984</i> .....	170
	<i>F. The Criminal Justice Act Extension</i> .....	171
III.	THE PRIVACY DEBATE.....	172
	<i>A. Development of the Right to Privacy in the United</i> <i>Kingdom</i> .....	172
	<i>B. NDNAD and Arrestee DNA Considered in Light of the</i> <i>Privacy Debate</i> .....	174
IV.	THE EUROPEAN COURT OF HUMAN RIGHTS’ DECISION IN <i>S &amp;</i> <i>MARPER V. UNITED KINGDOM</i> .....	180
V.	THE SUPREME COURT OF THE UNITED STATES’ DECISION IN <i>MARYLAND V. KING</i> .....	182
VI.	CONCLUSION.....	185

---

\* J.D., University of Georgia, 2014; B.S., Georgia Institute of Technology, 2009.

## I. INTRODUCTION

Since the discovery of DNA and its potential uses in the field of forensics, countries across the world have been trying to find ways to use DNA testing to their advantage. Often, this leads to unique and challenging legal questions. In the United States, arrestee DNA legislation has proven to be a controversial issue with just over half of U.S. states enacting laws for the purpose of creating and maintaining DNA databases, and half the states remaining without such laws.<sup>1</sup> Meanwhile, the federal government also collects arrestee DNA in certain cases.<sup>2</sup> In many states this type of legislation has been challenged as unconstitutional, despite advocates of such data collection consistently lobbying for it across the nation.<sup>3</sup> These challenges have resulted in split decisions amongst state and federal courts across the United States.<sup>4</sup>

Signaling the importance of the matter, the Supreme Court of the United States decided *Maryland v. King*, in which Maryland's arrestee DNA legislation was challenged as a violation of the Fourth Amendment's

---

<sup>1</sup> Julie Samuels et al., *Collecting DNA From Arrestees: Implementation Lessons*, 270 NAT'L INST. JUST. J. 18, 19 (2012).

<sup>2</sup> DNA Identification Act of 1994, 42 U.S.C. § 14132 (2006).

<sup>3</sup> See Samuels et al., *supra* note 1, at 19.

<sup>4</sup> See, e.g., *United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011) (finding that the collection of DNA from arrestees is constitutional, because arrestees have a diminished expectation of privacy); *United States v. Fricosu*, 844 F. Supp. 2d 1201 (D. Colo. 2012) (finding that arrestee DNA sample obtained upon probable cause for commission of a federal felony is constitutional); *United States v. Thomas*, 2011 U.S. Dist. LEXIS 45333 (W.D.N.Y. Feb. 14, 2011) (finding that "the government's interest in accurate and rapid identifications outweighs [the defendant's] privacy interest in the collection and analysis of a DNA sample"); *Haskell v. Brown*, 677 F. Supp. 2d 1187 (N.D. Cal. 2009), *aff'd sub nom. Haskell v. Harris*, 669 F.3d 1049 (9th Cir. 2012) (rejecting a motion to enjoin enforcement of California's arrestee DNA statute, noting that the plaintiffs were unlikely to succeed in establishing a Fourth or Fourteenth Amendment violation); *United States v. Pool*, 645 F. Supp. 2d 903 (E.D. Cal. 2009) (upholding the constitutionality of DNA sample collection from those arrested upon a judicial or grand jury determination of probable cause for the commission of a felony); *Mario W. v. Kaipio*, 281 P.3d 476 (Ariz. 2012) (taking DNA upon arrest involves two distinct intrusions on a juvenile's privacy); *People v. Buza*, 129 Cal. Repr. 3d 753 (2011), *transferred with direction to vacate*, 302 P.3d 1051 (2013) (holding the California DNA Act, in requiring felony arrestees to submit a DNA sample without independent suspicion, warrant, or grand jury determination of probable cause, is a violation of the Fourth Amendment); *In re Welfare of C.T.L.*, 722 N.W.2d 484 (Minn. Ct. App. 2006) (holding that the Minnesota DNA arrestee statute constitutes a violation of the Fourth Amendment); *Anderson v. Commonwealth*, 650 S.E.2d 702 (Va. 2007) (collecting DNA from someone arrested for a violent felony does not constitute a Fourth Amendment violation).

guarantee against unreasonable searches and seizures.<sup>5</sup> Petitioner Alonzo King challenged his conviction for rape, claiming that it was based on an unlawful search and seizure, as his DNA profile had been collected upon his arrest for a separate, unrelated crime.<sup>6</sup> In the majority opinion by Justice Kennedy, the Court held that the collection of a DNA sample upon arrest for a serious offense was reasonable under the Fourth Amendment.<sup>7</sup>

Still, the Court's opinion may be read quite broadly and does not answer all of the questions about DNA collection legislation in the United States. The debate forming around the collection and retention of DNA in the United States may be illuminated by the actions of other countries that have implemented similar laws. Many legislators attempt to strike a balance between citizens' rights to privacy and the legitimate state interests that are served by arrestee DNA sampling and retention as they make a foray into this area of forensic science. By taking note of what other countries have already tried and what other courts have already deemed acceptable or unacceptable, the United States could avoid some of the potential downfalls of DNA sampling and retention.

The first country to implement a DNA databank system was the United Kingdom, followed swiftly by other European nations and the United States.<sup>8</sup> The U.K. began collecting and maintaining DNA profiles in their National DNA Database (NDNAD) in 1995.<sup>9</sup> This database was, until very recently, the largest DNA database in the world, with roughly 5.5 million unique profiles collected as of March 1, 2012.<sup>10</sup> Proportionally, it is still the largest database in the world and, numerically, is second only to the United States' Combined DNA Index System (CODIS), which has over 6 million profiles

---

<sup>5</sup> 133 S. Ct. 1958 (2013).

<sup>6</sup> *Id.* at 1965.

<sup>7</sup> *Id.* at 1980. This case will likely have a lasting effect for decades to come and invites exploration of many Fourth Amendment issues, but the focus of this Note is on DNA collection and retention. It is for another day to explore the implications it will have on U.S. privacy law and criminal procedure.

<sup>8</sup> Duncan Carling, Note, *Less Privacy Please, We're British: Investigating Crime with DNA in the U.K. and the U.S.*, 31 HASTINGS INT'L & COMP. L. REV. 487, 492 (2008); INTERNATIONAL CRIMINAL POLICE ORGANIZATION, INTERPOL GLOBAL DNA SURVEY 2008 KEY FACTS (indicating that as of 2008, forty-two member-states employed a DNA database).

<sup>9</sup> Carling, *supra* note 8.

<sup>10</sup> Karen J. Maschke, *DNA and Law Enforcement*, in FROM BIRTH TO DEATH AND BENCH TO CLINIC: THE HASTINGS CENTER BIOETHICS BRIEFING BOOK FOR JOURNALISTS, POLICYMAKERS, AND CAMPAIGNS 45–50 (Mary Crowley ed., 2008).

collected.<sup>11</sup> Proponents of the widespread sampling of arrestee DNA profiles and databases often point to the U.K. as the leading example of how to best implement such systems and how advantageous they can be in aiding criminal investigations and preventing crime.<sup>12</sup>

There have been several studies performed in the United States documenting the purportedly advantageous uses of arrestee DNA databases.<sup>13</sup> One such study indicated that requiring the collection of DNA profiles upon felony arrest rather than felony conviction could have prevented sixty violent crimes, including fifty-three murders and rapes.<sup>14</sup> The study stressed that the eight convicted persons studied had twenty-one prior felony arrests between them, only seven of which were for violent crimes.<sup>15</sup> A similar Maryland study suggests obtaining DNA samples upon arrest of three individuals charged with a burglary, a sex offense, or a violent crime could have prevented twenty other crimes.<sup>16</sup> One can infer from these studies that in order for arrestee DNA sampling to best serve the public interest, sampling should not be limited to samples taken upon arrest for violent crimes, but should be extended to all felonies, as violent crimes are often committed by people who have previously been arrested for non-violent felonies. Undoubtedly, the collection, retention, and comparison of

---

<sup>11</sup> National DNA Database Statistics, <https://www.gov.uk/government/publications/national-dna-database-statistics> (last visited Nov. 11, 2013). As a point of clarity, the NDNAD actually contains roughly 5.6 million DNA profiles, but that number also includes approximately 1 million “duplicate” profiles from the same people, for various reasons, so the number of unique profiles in the system is approximately 4.8 million.

<sup>12</sup> Jay Siegel & Susan D. Narveson, *Why Arrestee DNA Legislation Can Save Indiana Taxpayers Over \$60 Million per Year*, 6–7 (Jan. 2009), available at [http://dnasaves.org/files/IN\\_DNA\\_Cost\\_Savings\\_Study.pdf](http://dnasaves.org/files/IN_DNA_Cost_Savings_Study.pdf).

<sup>13</sup> See CITY OF CHICAGO, *REQUIRING DNA FOR FELONY ARRESTS CAN SOLVE AND PREVENT VIOLENT CRIMES. WAITING FOR CONVICTION CAN COST LIVES* (2005), available at <http://www.dnasaves.org/files/ChicagoPreventableCrimes.pdf> [hereinafter CHICAGO STUDIES]; MARYLAND CRIMINAL JUSTICE INFO. SYS., BALTIMORE CTY. POLICE DEP'T & MARYLAND STATE POLICE, *REQUIRING DNA FOR QUALIFYING ARRESTS IN THE PROPOSED LEGISLATION CAN SOLVE AND PREVENT VIOLENT CRIMES* (2008), available at [http://www.denverda.org/DNA\\_Documents/Arrestee\\_Database/MarylandDNAarresteestudy.pdf](http://www.denverda.org/DNA_Documents/Arrestee_Database/MarylandDNAarresteestudy.pdf) [hereinafter MARYLAND STUDY]; WASHINGTON STATE PREVENTABLE CRIME STUDY (2008), available at [http://www.dnasaves.org/files/WASHINGTON\\_STATE\\_PREVENTABLE\\_CRIME.pdf](http://www.dnasaves.org/files/WASHINGTON_STATE_PREVENTABLE_CRIME.pdf); DENVER DISTRICT ATTORNEY'S OFFICE, *REQUIRING DNA FOR FELONY ARRESTS CAN SOLVE AND PREVENT VIOLENT CRIMES* (2009), available at [http://www.denverda.org/DNA\\_Documents/Denver's%20Preventable%20Crimes%20Study.pdf](http://www.denverda.org/DNA_Documents/Denver's%20Preventable%20Crimes%20Study.pdf).

<sup>14</sup> See CHICAGO STUDY, *supra* note 13.

<sup>15</sup> *Id.*

<sup>16</sup> See MARYLAND STUDY, *supra* note 13.

arrestee DNA samples would provide a significant advantage in criminal investigations and potentially in preventing crime.

While widespread DNA sampling can serve as an important tool in fighting crime, it can also create tension with human rights concerns. In late 2008, the European Court of Human Rights (the ECtHR) declared the U.K.'s widespread collection and indefinite retention of arrestee DNA samples to be a violation of the European Convention on Human Rights.<sup>17</sup> Even prior to this holding, many human rights activists and commentators had expressed concern about the potential violations of privacy that were occurring in the U.K.<sup>18</sup> Additionally, there were concerns that the U.K. databases were being used to perpetuate racial discrimination. Further, commentators noted the databases' potential for future misuse, including accessing the stored information for purposes other than criminal investigations.<sup>19</sup> Finally, statistics showed that the DNA profiles of many people who had either been acquitted or never been charged in the first place remained in the databanks, with authorities refusing to delete them. All of these concerns were brought to light in the ECtHR's 2008 ruling.

The purpose of this Note is to provide a comprehensive overview of the developments in U.K. law in the field of forensic DNA databasing in light of the United States' recent foray into this area. As such, this Note will examine the debate that surrounded the drafting and implementation of the U.K.'s various statutes that allow for such widespread sampling and retention of DNA profiles. Part II will focus on the particular statutes and amendments that expanded DNA profile collection in the U.K. Specifically, U.K. legislators adhered to no overarching legislative scheme; rather, the ability to collect DNA profiles expanded over a number of years by way of piecemeal legislation that gradually increased the police power to obtain and retain DNA profiles.<sup>20</sup> Part III will turn to the discourse that surrounded the

---

<sup>17</sup> S. & Marper v. United Kingdom, [2009] Eur. Ct. H.R. (1581).

<sup>18</sup> GENEWATCH UK, THE POLICE NATIONAL DNA DATABASE: BALANCING CRIME DETECTION, HUMAN RIGHTS AND PRIVACY 38–46 (2005), available at <http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/NationalDNADatabase.pdf>.

<sup>19</sup> *Id.* at 12.

<sup>20</sup> See generally ROYAL COMMISSION ON CRIMINAL JUSTICE, REPORT, 1993, cm. 2263, ¶¶ 36–38 (U.K.) [hereinafter ROYAL COMMISSION REPORT] (recommending DNA database); Criminal Justice and Public Order Act, 1994, c. 33, § 172 (U.K.) (establishing National DNA Database); Criminal Evidence (Amendment) Act, 1997, c. 17, §§ 1–3 (U.K.) (allowing for non-intimate sample to be taken from persons who committed a violent crime, sex offense, or burglary prior to 1995); Criminal Justice and Police Act, 2001, c. 16 (U.K.) (allowing for the indefinite retention of samples and fingerprints); Criminal Justice Act, 2003, c. 44 § 10 (U.K.)

passing of those statutes and amendments, with a particular focus on how the legislature conceptualized individual privacy rights and sought to balance those rights with the original state interests. Part IV will analyze the ECtHR's decision in the case of *S. & Marper v. United Kingdom*, where the Court held that the indefinite retention of arrestee DNA profiles violated the Human Rights Act of 1998. In its analysis, the Court applied a balancing test, attempting to strike the correct proportion between privacy protection and advancing state interests in crime prevention.<sup>21</sup> Finally, Part V of this Note will examine the Supreme Court of the United States' recent decision in *Maryland v. King* and how this opinion differs from that of the European Court of Human Rights. This retrospective look at the United Kingdom's initial venture into the world of DNA databasing provides a comprehensive view of the various downfalls to avoid as the federal and state governments within the U.S. attempt to refine their laws and employ DNA database systems to their fullest capabilities, while simultaneously protecting what privacy rights their citizens have. In light of the recent Supreme Court decision, it appears as if the U.S. may have just taken the first step down a road already traveled.

#### *A. Background on Forensic DNA Analysis*

In order to understand many of the topics and concepts embodied in this Note, it is important to understand the mechanisms of forensic DNA sampling and use. In 1985, Professor Alec Jeffreys of Leicester University developed a method by which "patterns of chemical signals within the DNA molecule" that are unique to each person could be identified and recorded.<sup>22</sup> This form of identification, known as a DNA profile, soon began to be recognized as a valuable tool in aiding criminal investigations and other situations where determining identity was relevant, such as paternity suits.

In modern criminal investigations, DNA evidence is considered biological physical evidence.<sup>23</sup> When DNA sampling and analysis was first used in this capacity, the early technology required a sizeable sample of bodily fluid, such as semen or blood, in order to obtain a satisfactory

---

(allowing samples to be taken from any person arrested for a "recordable offence"—or any offence which could result in imprisonment).

<sup>21</sup> See *S. & Marper*, [2008] Eur. Ct. H.R. 1581 at n.16.

<sup>22</sup> Andrew Hall, *DNA Fingerprints – Black Box or Black Hole?*, 140 NEW L.J. 203 (Feb. 1990).

<sup>23</sup> See GENEWATCH UK, *supra* note 18, at 11.

profile.<sup>24</sup> Today, with advances in DNA technology, analysts can often use a technique known as “touch DNA” to generate a full profile with as few as twenty dead skin cells.<sup>25</sup>

There are three main types of DNA analysis currently used to aid forensic investigations: nuclear DNA analysis, mitochondrial DNA analysis, and Y-Chromosome analysis.<sup>26</sup> In all forms of DNA analysis, the process of generating a DNA profile includes obtaining a piece of evidence likely to contain DNA, isolating the DNA from that evidence, and then processing the DNA to obtain a series of markers known as the DNA profile.<sup>27</sup> The markers are indicative of various alleles present at different locations (known as loci) in the DNA chain, or genome.<sup>28</sup>

Current forensic DNA testing in the United States focuses on short tandem repeat (STR) analysis, a form of nuclear DNA testing.<sup>29</sup> In this type of analysis, analysts evaluate specific loci found in nuclear DNA and create a DNA profile that consists of thirteen loci in the DNA chain.<sup>30</sup> The chances of any two people (who are not identical twins) having the exact same thirteen loci DNA profile is estimated to be as high as one in one billion or more.<sup>31</sup> While thirteen is the optimal number of loci, the FBI currently only requires a profile with ten identified loci in order for that profile to be uploaded into the National DNA Index System (NDIS) for forensic purposes.<sup>32</sup>

Furthermore, the chain of markers used in forensic DNA identifications is what is commonly referred to as “junk DNA.”<sup>33</sup> That is, it does not involve the full amount of information that a DNA sample could potentially hold about an individual and thus is an unnecessarily limited use of DNA sampling. For instance, the DNA “fingerprints” used by criminal

---

<sup>24</sup> *Id.* at 26.

<sup>25</sup> *Touch DNA*, DNA FORENSICS, available at <http://www.dnaforensics.com/touchdna.aspx>.

<sup>26</sup> *DNA Evidence: Basics of Analyzing*, NAT'L INST. OF JUST., <http://www.nij.gov/nij/topics/forensics/evidence/dna/basics/analyzing.htm> (last visited Oct. 11, 2013).

<sup>27</sup> *Id.*

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, FED. BUREAU OF INVESTIGATION, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet> (last visited Oct. 11, 2013) [hereinafter *CODIS FAQs*].

<sup>33</sup> NATIONAL INSTITUTE OF JUSTICE, THE FUTURE OF FORENSIC DNA TESTING, PREDICTIONS OF THE RESEARCH AND DEVELOPMENT WORKING GROUP 12 (2000), available at <https://www.ncjrs.gov/pdffiles1/nij/183697.pdf>.

investigators today contain information about gender and the specific chain of markers can be used as an identifier, but they do not contain information about appearance, health, and behavior.<sup>34</sup> These pieces of information can, however, be found elsewhere in the genome, which has sparked some of the controversy surrounding forensic DNA sampling.<sup>35</sup>

For the purposes of this Note, it is also important to understand the distinction between a DNA sample and a DNA profile. A sample is the physical specimen collected in order to generate a profile, i.e., blood, semen, saliva, or skin cells.<sup>36</sup> A profile, on the other hand, refers to the string of numbers indicating which alleles are present at the loci.<sup>37</sup> The profile is generated by a DNA analysis of the sample. While a DNA profile derived from the so-called junk DNA may not contain much more than identifying information, a DNA sample may have much more information available for analysis.<sup>38</sup>

## II. THE U.K. LEGISLATION

The legislation that led the U.K. to the decision in *S. & Marper v. United Kingdom* was not formed pursuant to some overarching legislative scheme. On the contrary, the system, which came to govern the input and maintenance of samples and profiles in the NDNAD, came about as a result of several different pieces of legislation passed over the course of a decade.<sup>39</sup> Each contributing piece of legislation is examined in more in depth, beginning with the Recommendation of the Royal Commission on Criminal Justice, which was the first body to recommend the establishment of a DNA database and the use of DNA testing to aid criminal investigations. Each section will also discuss what concerns, if any, were espoused about the protection of privacy rights, or what general wariness was expressed at the rapidly expanding system.

---

<sup>34</sup> *Id.* at 61.

<sup>35</sup> *Id.*

<sup>36</sup> ANDREI SEMIKHODSKII, DEALING WITH DNA EVIDENCE: A LEGAL GUIDE 23 (2007).

<sup>37</sup> See *CODIS FAQs*, *supra* note 32.

<sup>38</sup> *Id.*

<sup>39</sup> See discussion *infra* Part II.A–II.E.



*A. The Royal Commission on Criminal Justice's 1993 Recommendation*

In 1993, the Royal Commission on Criminal Justice recommended that the U.K. employ a DNA database.<sup>40</sup> Their primary goal in adopting the database was to achieve a “more objective form of forensic identification.”<sup>41</sup> The Commission’s recommendation came as a result of several high-profile cases involving quashed convictions that ignited public debate about the criminal system and its effectiveness in achieving justice.<sup>42</sup> The original intent behind establishing a DNA database was to obtain a more reliable way not only to secure convictions but also to narrow the field of suspects during a criminal investigation.<sup>43</sup> The Commission also recommended that police should be able to take non-intimate DNA samples from those arrested for serious crimes and that clear legislation was necessary to provide for more extensive storage of DNA, both for the purposes of identifying offenders and for keeping a database.<sup>44</sup> The recommendation further stated that samples could be obtained from those accused of serious offenses even where DNA evidence was irrelevant to the offense, and such DNA could be retained for further use if that person were to be convicted.<sup>45</sup>

The overall report of the Commission was lengthy, with numerous recommendations for the improvement of the criminal justice system as a whole.<sup>46</sup> As a result, these two specific points were in large part overlooked as they constituted some of the more minor recommendations of the Commission. Public discourse seemed to focus on the Commission’s proposed Criminal Cases Review Authority, which was a body made up of lay members and lawyers and was intended to investigate alleged miscarriages of justice.<sup>47</sup>

---

<sup>40</sup> ROYAL COMMISSION REPORT, *supra* note 20, ¶¶ 35–38.

<sup>41</sup> GENEWATCH UK, *supra* note 23, at 26.

<sup>42</sup> Terry Kirby & Heather Mills, *Royal Commission on Criminal Justice: Reformers Applaud Proposal for Body to Review Cases: New Authority Would Examine Possible Miscarriages of Justice*, INDEPENDENT, July 7, 1993.

<sup>43</sup> See Carling, *supra* note 8.

<sup>44</sup> See ROYAL COMMISSION REPORT, *supra* note 20, ¶ 33.

<sup>45</sup> *Id.* ¶ 34.

<sup>46</sup> See generally *id.* (calling for researching jurors’ reasoning, reforming identification procedures, setting guidelines for witness and victim interviews, among other recommendations).

<sup>47</sup> See John Wadham, *Unravelling Miscarriages of Justice*, 143 NEW L.J. 1650 (1993); Siobhan M. Keegan, *The Criminal Cases Review Commission’s Effectiveness in Handling Cases From Northern Ireland*, 22 FORDHAM INT’L L.J. 1776, 1801 (1999).

*B. The Criminal Justice and Public Order Act*

In 1994, the NDNAD was established by the Criminal Justice and Public Order Act.<sup>48</sup> In addition to establishing the NDNAD, this Act also amended the definitions of intimate and non-intimate samples: classifying saliva, swabs from any part of the body that is not an orifice, and non-pubic hair as non-intimate samples.<sup>49</sup> Significantly, different protocols governed the collection of intimate and non-intimate samples; samples that were considered non-intimate were easier to obtain. Amending the definitions had the effect of allowing for the sampling of various substances that would contain DNA on the basis that they were now considered non-intimate samples. The division between intimate and non-intimate samples appears to focus on the amount of physical invasion as opposed to the amount of information gathered.

According to the amended definitions, intimate samples included “a) . . . blood, semen, or any other tissue fluid, urine or pubic hair; b) a dental impression; and c) a swab taken from a person’s body orifice other than the mouth.”<sup>50</sup> Arguably, one’s DNA profile contains much more information about oneself than does a dental impression or even a fingerprint, since dental impressions and fingerprints can only provide identification information and DNA samples may contain information about race, sex, family, and genetic disorders.<sup>51</sup> The DNA sample, however, can be obtained by less obtrusive means. For example, using current technology, a DNA profile could be obtained with as few as twenty dead skin cells; obtaining a sufficient sample size would be as simple as swabbing someone’s hand—which is arguably even less physically invasive than a typical buccal (oral) swab, dental impression, or collection of any type of bodily fluid, as it does not require entry into any orifice.

Additionally, under this portion of the Act, there were still provisions for the destruction of evidence, as well as restrictions as to how and when the collected samples could be used in evidence.<sup>52</sup> As discussed below, many of the provisions for destruction of samples were slowly eroded over time. This

---

<sup>48</sup> Criminal Justice and Public Order Act, *supra* note 20, § 60A.

<sup>49</sup> *Id.* § 58(3).

<sup>50</sup> *Id.* § 58(2).

<sup>51</sup> See *DNA Evidence: Basics of Analyzing*, *supra* note 26.

<sup>52</sup> See Criminal Justice and Public Order Act, *supra* note 20, § 57.

is noteworthy, because indefinite retention of samples was one of the main issues the *Marper* court was concerned about.<sup>53</sup>

### C. *The Criminal Evidence (Amendment) Act*

In 1997, an amendment to the Criminal Evidence Act extended the police power to allow the collection of non-intimate body samples from certain convicts without their consent.<sup>54</sup> That is, non-intimate samples (as previously defined by the Criminal Justice and Public Order Act) could be collected from persons convicted and detained at the time of enactment for certain offenses, including any sex crime, violent crime, or burglary that had been committed before the establishment of the NDNAD.<sup>55</sup> This amendment also allowed for the collection of non-intimate samples from children and the mentally ill at the places where they were detained, provided they met the requirements for the collection of the sample.<sup>56</sup>

The amendment enabled the collection of DNA samples from approximately 7,750 sexual offenders, violent offenders, and burglars; their profiles were subsequently put into the NDNAD.<sup>57</sup> These changes to the Criminal Evidence Act stemmed directly from the recommendations of the Royal Commission.<sup>58</sup> This bill was enacted for the purpose of “plug[ging]” the “loophole” left by its predecessor, namely the lack of any provision allowing for the collection of DNA samples from anyone convicted before April 10, 1995.<sup>59</sup>

After some discussion in Parliament of the excellent advances in criminal investigations directly attributable to the NDNAD and advances in DNA technology, this bill was accepted with support from all sides of the House.<sup>60</sup> In advancing the bill, Mr. Nigel Evans of the House of Lords noted six benefits, including “the early identification of linked cases, the early arrest of offenders, valuable intelligence, early exoneration of innocent suspects, easier identification of bodies and, finally, deterrence.”<sup>61</sup> Mr. Evans also made note of the potential usefulness of a DNA database in solving so-called

---

<sup>53</sup> See *S. & Marper*, *supra* note 17.

<sup>54</sup> Criminal Evidence (Amendment) Act, *supra* note 20, §§ 1–3.

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> 290 PARL. DEB., H.C. (6th ser.) (1997) 1029-30 (U.K.).

<sup>58</sup> 578 PARL. DEB., H.L. (5th ser.) (1997) 105-112 (U.K.).

<sup>59</sup> *Id.* at 110.

<sup>60</sup> *Id.* at 112.

<sup>61</sup> 288 PARL. DEB., H.C. (6th ser.) (1997) 1230-31 (U.K.).

“cold cases,” linking those already convicted of one crime to another, as yet unsolved, offense.<sup>62</sup>

These six reasons comport fully with all of the reasons advanced by current supporters of DNA sampling of arrestees and have been found by courts to be compelling state interests.<sup>63</sup> In a follow-up statement, Mr. Kirkhope, the Parliamentary Under-Secretary of State for the Home Department, spoke at length on the six aforementioned interests served by expanding DNA sampling.<sup>64</sup> Mr. Kirkhope also spoke of “safeguarding . . . the interests of innocent members of the public,” mentioning the security of the DNA database, and the ability of DNA science to help eliminate innocent suspects while simultaneously identifying perpetrators.<sup>65</sup> While he further noted that there is a possibility of error, Mr. Kirkhope asserted that the benefits of expanding DNA testing outweighed any potential mistakes or undesirable consequences in light of the precautions taken by the Forensic Science Service, such as double testing samples when a match is reported and extensive safeguards against contamination of samples.<sup>66</sup>

#### *D. The Data Protection Act of 1998*

The Data Protection Act, though it does not relate directly to the operation of the NDNAD, specifies a number of “protection principles” that must be met when certain types of personal data are collected and stored. Three principles in particular are highly relevant to the topic of DNA collection and retention. Notably: “Personal data shall be adequate, relevant, and *not excessive* in relation to the purpose or purposes for which they are processed”; data should not be kept for any time period longer than necessary to achieve the purpose it was obtained for, and measures should be taken to guard against the unlawful processing of personal data.<sup>67</sup> Of particular importance is the principle that data obtained for a particular purpose shall only be retained for as long as necessary to achieve that purpose.<sup>68</sup> This provision is in direct conflict with the requirement adopted

---

<sup>62</sup> *Id.*

<sup>63</sup> *Haskell v. Harris*, 669 F.3d 1049, 1063–64, *reh'g en banc granted*, 686 F.3d 1121 (9th Cir. 2012); *United States v. Mitchell*, 652 F.3d 387, 404 (3d Cir. 2011); *Why Pass the DNA Law?*, DNA SAVES, [http://dnasaves.org/dna\\_law.php](http://dnasaves.org/dna_law.php) (last visited Oct. 11, 2013).

<sup>64</sup> See PARL. DEB., H.C., *supra* note 61, at 1233–36.

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> Data Protection Act, 1998, c. 29, sch. 1 (Eng.) (emphasis added).

<sup>68</sup> *Id.*

in the Police and Criminal Evidence Act Amendment that allows for the indefinite retention of DNA profiles and samples.<sup>69</sup>

Furthermore, this Act was explicitly considered and passed in light of the adoption of the European Convention on Human Rights (Convention).<sup>70</sup> During the Parliamentary debates on this particular bill, Baroness Nicholson in the House of Lords discussed at length the fact that the U.K. had no express right to privacy, which many of its citizens may have assumed they had. She noted the arguments of Lord Lester, who claimed that in incorporating the Convention, the U.K. had a “positive obligation” to create a right of privacy.<sup>71</sup>

Mr. Lester’s comments arose during the debates surrounding a particular clause of the Act that would greatly expand the police power.<sup>72</sup> He proposed that rather than relying on the dovetailing of U.K. common law with the provisions of Article 8 of the Convention, it would be more desirable for Parliament to affirmatively create a right to privacy.<sup>73</sup> This, he argued, was preferable to leaving that obligation to the courts, where they would be forced to interpret the law, carving out a common law right of privacy.<sup>74</sup>

Mr. Lester further questioned the Solicitor-General as to whether the adoption of the bill as-is would in fact violate Article 8 of the Convention.<sup>75</sup> The confusing response was that the bill itself would constitute no such violation, but that any order pursuant to the bill would have to be considered in light of the Convention, and that the Government must be trusted to exercise good faith in adhering to the principles of both.<sup>76</sup> Put simply: the response to concerns about the U.K.’s ability to comply with Article 8 of the Convention without first establishing a statutory right to privacy in Parliament was that they should “accept not only the Government’s good faith, but whatever decision they reach” when a question arose under the Convention.<sup>77</sup>

---

<sup>69</sup> Police and Criminal Evidence Act (PACE) 1984, c. 60, § 642k (U.K.).

<sup>70</sup> 585 PARL. DEB., H.L. (5th ser.) (1998) 436 (U.K.).

<sup>71</sup> *Id.* at 450.

<sup>72</sup> In a letter to Baroness Nicholson, the Data Registrar indicated that the debated clause was “unprecedented” and would operate in such a way as to take away protections given by the previous Data Protection Act of 1984. 587 PARL. DEB., H.L. (5th ser.) (1998) 1099 (U.K.).

<sup>73</sup> *Id.* at 1096.

<sup>74</sup> *Id.*

<sup>75</sup> *Id.* at 1103.

<sup>76</sup> *Id.* at 1103-04.

<sup>77</sup> *Id.* at 1105.

*E. The Police and Criminal Evidence Act of 1984*

In 2001, the Police and Criminal Evidence Act 1984 (PACE), was extended by the Criminal Justice and Police Act 2001 (CJPO 2001).<sup>78</sup> One of the most significant changes that resulted from this extension was that it allowed for the indefinite retention of all DNA samples and fingerprints, where PACE had originally expressly prohibited such retention.<sup>79</sup> The CJPO only applied to England and Wales; Scotland and Northern Ireland remained free to destroy samples of those acquitted or those against whom the charges had been dropped.<sup>80</sup>

Additionally, the samples of consenting volunteers who took part in mass screenings would be retained indefinitely as well.<sup>81</sup> Samples from volunteers or those otherwise consenting to retention need not be destroyed pursuant to other sections of the Act and had no restrictions upon the purpose for which they may be used.<sup>82</sup> Further, consent could not be withdrawn.<sup>83</sup> In a sense, samples that were voluntarily given were provided with less protection than those obtained from suspected criminals.

As a purportedly limiting measure, Section 82(2)(1A)(b) of the Act provides that retained samples “shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.”<sup>84</sup> As noted above, this conflicts with the requirements of the 1998 Data Protection Act. Under that statute, once a person has been acquitted of the crime with which they were charged and the investigation is no longer ongoing, their personal information should be purged from the system entirely. It was this section in particular that would eventually lead to challenges under Articles 8 and 14 of the European Convention on Human Rights.<sup>85</sup>

The difference between the number of samples destroyed or removed from the database before and after the enactment of CJPO 2001 is startling. From 1999 to 2001, 137,293 records were removed from the database,

---

<sup>78</sup> Criminal Justice and Police Act, *supra* note 20.

<sup>79</sup> Jason M. Swergold, Note, *To Have and to Hold: The Future of DNA Retention in the United Kingdom*, 33 B.C. INT'L & COMP. L. REV. 179, 184 (2010).

<sup>80</sup> See Criminal Justice and Police Act, *supra* note 20 (applying the CJPO only to England and Wales).

<sup>81</sup> *Id.* § 82(4)(3AC).

<sup>82</sup> *Id.*

<sup>83</sup> *Id.*

<sup>84</sup> *Id.* § 82(2)(7A)(b).

<sup>85</sup> Charles Bourne, *Retaining Fingerprints and DNA Samples*, 152 NEW L.J. 1693 (2002).

compared to only 70,035 records removed from 2001 to 2004.<sup>86</sup> Samples may have been destroyed and profiles removed from the NDNAD for the following reasons: the individual died; the samples were taken in error; the individual was acquitted or the charges against him were dropped; or the records were duplicates.<sup>87</sup>

In December 2003, an estimated 109,000 profiles belonging to those who had been acquitted remained in the NDNAD.<sup>88</sup> Of those who had voluntarily given their DNA samples, approximately 10,500 profiles were in the database.<sup>89</sup> This subset primarily includes people who were asked to provide a sample as a result of an intelligence screening exercise conducted by law enforcement when an offender was believed to live nearby.<sup>90</sup>

#### *F. The Criminal Justice Act Extension*

Finally, in April 2004, certain provisions of the Criminal Justice Act 2003 went into force, allowing for the collection and indefinite retention of samples from all persons arrested for any “recordable offense” who had been taken to a police station in connection with that offense.<sup>91</sup> In other words, regardless of whether a person was ever charged or convicted, his or her DNA sample was obtained once he or she was detained at the police station, and that sample could be kept and cross-referenced indefinitely.

In the Parliamentary debates surrounding this extension, an amendment allowing for the destruction of samples and fingerprints in certain situations was considered and rejected.<sup>92</sup> In arguing against the amendment, Baroness Scotland, then Minister of State for the Criminal Justice System and Law Reform, took note of the approximately 103,000 DNA profiles in the NDNAD which would have previously been deleted from the system due to an acquittal.<sup>93</sup> Of these, over 4,500 profiles were matched to crime scene samples, including the samples taken from “26 murders, 15 attempted murders, 27 rapes, 13 sexual offences, 14 aggravated burglaries and six of the supply of controlled drugs.”<sup>94</sup> She used these statistics to argue that

---

<sup>86</sup> 420 PARL. DEB., H.C. (6th ser.) (2004) 1295, 1296W (U.K.).

<sup>87</sup> *Id.*

<sup>88</sup> 415 PARL. DEB., H.C. (6th ser.) (2003) 616W (U.K.).

<sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> Criminal Justice Act, 2003, c. 44 (U.K.).

<sup>92</sup> 654 PARL. DEB., H.L. (5th ser.) (2003) 1940-41 (U.K.).

<sup>93</sup> *Id.*

<sup>94</sup> *Id.* at 1941.

reverting back to a system that deleted the DNA profiles of acquitted persons would be an undesirable step backwards in the use of DNA as an investigative tool. Still, this argument disregards the approximately 99,000 profiles of acquitted persons that were never matched to any sort of crime or criminal investigation.<sup>95</sup>

### III. THE PRIVACY DEBATE

In the late 1990s and early 2000s all these pieces of legislation enjoyed a great deal of public support. The public had professed general safety concerns and, on the whole, people seemed concerned about the police not catching the right criminals or not catching as many criminals as they could.<sup>96</sup> In fact, in 1994 the Secretary of State for the Home Department commented on the establishment of protocols for collecting DNA samples for criminal investigations:

Almost all the correspondence we have received has been supportive of our proposals to allow DNA samples to be taken in all recordable offences. The police have warmly welcomed our plans. They help bring the law into line with the capabilities of modern technology. The full force of modern science will be brought to bear upon the modern criminal.<sup>97</sup>

However, as early as 2002 the tides of public opinion began to shift as DNA technology rapidly advanced and the databanks began to expand. Human rights groups in particular expressed growing concern about the future of DNA testing and privacy rights, including how the databanks would or could be misused in the future, given that the U.K. did not until very recently have a recognized right to privacy.<sup>98</sup>

#### *A. Development of the Right to Privacy in the United Kingdom*

U.K. common law does not recognize a right to privacy.<sup>99</sup> Some commentators have extrapolated from this that because there had been no

---

<sup>95</sup> *Id.*

<sup>96</sup> ROYAL COMMISSION REPORT, *supra* note 20, at 10.

<sup>97</sup> 248 PARL. DEB., H.C. (6th ser.) (1994) 1335-36 Wf (U.K.).

<sup>98</sup> See text at *supra* Part II.A.

<sup>99</sup> *Kaye v. Robertson*, [1991] F.S.R. 62.



statutory or otherwise enumerated right to privacy the NDNAD could not possibly have violated such a right.<sup>100</sup> However, this statement ignores the implication of the Human Rights Act of 1998, which formally incorporated the European Convention on Human Rights into U.K. law.<sup>101</sup> Article 8 of the Convention explicitly states: “Everyone has the right to respect for his private and family life.”<sup>102</sup> The Convention was integrated into U.K. law the same year that the Data Protection Act was passed, and a mere four years after the establishment of the NDNAD.<sup>103</sup> The adoption of both of these statutes indicates an awareness and acceptance on the part of Parliament that citizens do have some sort of privacy right and that certain precautions should be taken in order to avoid violating that right.<sup>104</sup>

Furthermore, questions about a right to privacy in the U.K. arose in many different contexts even before the adoption of the Convention.<sup>105</sup> Notably, the notion of an officially recognized right to privacy first experienced a great deal of discussion in England in the context of paparazzi and famous figures.<sup>106</sup> Many of the arguments against recognizing a separate right to privacy revolved around the notion that such a right was already protected by the law of confidence.<sup>107</sup> The law of confidence, briefly put, protects private information from being publicly disseminated to the detriment of the party whom the information concerns.<sup>108</sup> Others argued that the law of confidence, though it provided protection in some areas, did not go far enough.<sup>109</sup> One such proponent, Lord Keith, stated that “the right to personal privacy is clearly one which the law should in this field seek to protect.”<sup>110</sup>

---

<sup>100</sup> See generally Carling, *supra* note 8 (illustrating the differences between the U.K. and the U.S. law, particularly cultural views of the right to privacy).

<sup>101</sup> Human Rights Act, 1998, c. 42 (U.K.); Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221 [hereinafter Convention].

<sup>102</sup> Convention, *supra* note 101, art. 8.

<sup>103</sup> Human Rights Act, *supra* note 101 (enacted in 1998); Data Protection Act, *supra* note 67 (enacted in 1998); Criminal Justice and Public Order Act, *supra* note 20 (enacted in 1994).

<sup>104</sup> See text at *supra* Part II.D.

<sup>105</sup> Jonathan Morgan, *Privacy, Confidence and Horizontal Effect: “Hello” Trouble*, 62 CAMBRIDGE L.J. 444 (2003).

<sup>106</sup> *Id.*

<sup>107</sup> E.g., Patrick Milmo, *Confidence and Privacy*, 143 NEW L.J. 1629 (1993) (illustrating some of the strengths and weaknesses of confidence law in protecting privacy).

<sup>108</sup> *Attorney General v. Observer Ltd.*, [1990] 1 A.C. 109.

<sup>109</sup> See text at *supra* Part II.A.

<sup>110</sup> Milmo, *supra* note 107.

The right to privacy was discussed in other contexts as well. In the context of sophisticated surveillance techniques such as software that logs keystrokes used to monitor employees in the workplace, one commentator from the U.K. noted that “[i]n a democratic society, privacy remains a basic right of citizens.”<sup>111</sup> Of course, she adds that there will always be conflict among enumerated rights—the difficulty lies in determining the correct balance.<sup>112</sup> Thus, the question of privacy rights and the correct balance to be struck concerning those rights was still open at the time that legislation regarding DNA databases was adopted.

*B. NDNAD and Arrestee DNA Considered in Light of the Privacy Debate*

Around 2002, the debate about the potential of arrestee DNA samples to constitute privacy intrusions began to intensify. There was some public concern that DNA profiles were not used to their full advantage, which is indicated in the legislative history of the extension of the Police and Criminal Evidence Act 1984.<sup>113</sup> This concern stemmed primarily from two cases in which DNA evidence was able to link suspects to a rape and a murder. In those cases, the DNA profiles were not able to be used against the suspects because the offenses which led to their collection failed to result in a conviction.<sup>114</sup>

In direct contrast, however, was growing concern on the part of human rights groups that the expanding use of DNA samples was, or could be, a violation of privacy.<sup>115</sup> After acknowledging that Article 8 of the Convention allowed for a recognized right to privacy, many were of the opinion that the use and retention of DNA samples did not violate that right. Section 8(2) states, in part, that no public authority should interfere with the right to respect for a private life “except such as is in accordance with the law and is *necessary* in a democratic society in the interests of national security, public safety . . . [or] *for the prevention of disorder or crime.*”<sup>116</sup> The argument was that since the express goal of the systematic collection of DNA was crime prevention, there was no violation of the Convention.

---

<sup>111</sup> Orla Ward, *Is Big Browser Watching You?*, 150 NEW L.J. 1414 (2000).

<sup>112</sup> *Id.*

<sup>113</sup> *S. & Marper v. United Kingdom*, 1581 Eur. Ct. H.R. at 15.

<sup>114</sup> *Id.*

<sup>115</sup> See generally GENEWATCH UK, *supra* note 23; *New Police Powers Unveiled*, BBC NEWS (Jan. 19, 2001, 14:27 GMT), [http://news.bbc.co.uk/2/hi/uk\\_news/politics/1125655.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/1125655.stm).

<sup>116</sup> Convention, *supra* note 101 (emphasis added).

In 2002, Baroness Hale disagreed with the holding of the House of Lords in the case of *S. & Marper v. United Kingdom*.<sup>117</sup> She indicated in her dissent that the retention of both fingerprints and DNA data constituted a violation of a person's right to a private life.<sup>118</sup> Information about an individual's genetic make-up, she reasoned, could be the absolute most private information one could possibly obtain about a person.<sup>119</sup> However, she agreed with the majority opinion that the government had provided sufficient justifications for the use and retention of DNA information in that particular case.<sup>120</sup>

Also in 2002, there were growing concerns about the ethnic makeup of the samples retained by the NDNAD. Notably, ethnic minorities were disproportionately represented in the NDNAD, indicating that the database may be biased against minorities who tend to make up the majority of the convicted population.<sup>121</sup> There were several proposals for how to combat this apparent discrimination. The inventor of the DNA fingerprint was reportedly alarmed at the discriminatory practices that surrounded the use of his technique, and called for the creation of a national database that would store the profiles of every citizen in the U.K.<sup>122</sup>

In her comment in the *New Law Journal* in 2002, B. Mahendra also argued that the most effective way to battle a disproportionate (and thus seemingly discriminatory) amount of minorities in the NDNAD was to institute a national DNA database and to incorporate national genetic identity cards.<sup>123</sup> Mahendra brushed off "slippery slope" type arguments, saying that to give credence to such arguments is to remain "blind to the workings of the modern world."<sup>124</sup> However, Mahendra's argument holds little water. First, she writes that one should lay aside any ethical or moral arguments concerning invasions of privacy and preservation of civil liberties.<sup>125</sup> Later,

---

<sup>117</sup> *S. & Marper*, 1581 Eur. Ct. H.R. at 25.

<sup>118</sup> *Id.* (Baroness Hale, dissenting).

<sup>119</sup> *Id.*

<sup>120</sup> *Id.*

<sup>121</sup> NUFFIELD COUNT OF BIOETHICS, THE FORENSIC USE OF BIOINFORMATION: ETHICAL ISSUES 56–57 (2007), available at <http://www.nuffieldbioethics.org/sites/default/files/The%20forensic%20use%20of%20bioinformation%20-%20ethical%20issues.pdf> [hereinafter NUFFIELD REPORT].

<sup>122</sup> *Privacy Fears over DNA Database*, BBC NEWS (Sept. 12, 2002), [http://news.bbc.co.uk/2/hi/in\\_depth/sci\\_tech/2002/Leicester\\_2002/2252782.stm](http://news.bbc.co.uk/2/hi/in_depth/sci_tech/2002/Leicester_2002/2252782.stm).

<sup>123</sup> B. Mahendra, Comment, *Citizens, DNA and Civil Liberties*, 152 NEW L.J. 1405 (Sept. 2002).

<sup>124</sup> *Id.*

<sup>125</sup> *Id.*

however, she claims there is no convincing argument based on civil liberties against a national database.<sup>126</sup> According to her, citizens have a “right to justice and the duty not merely to assist the authorities but also [their] fellow citizens,” and it is these rights and duties that trump any right to privacy.<sup>127</sup>

In early 2005, GeneWatch U.K. issued a report proposing limitations on the use and functions of the NDNAD, as there were serious concerns about future misuses of the system.<sup>128</sup> The concerns included discrimination,<sup>129</sup> ‘function creep,’<sup>130</sup> expansion of the databank to include the entire population,<sup>131</sup> increasing “back door” use of DNA databases that were initially established for health or research purposes,<sup>132</sup> and the possible linkage of multiple government databases.<sup>133</sup> On the subject of retaining the profiles and samples from unconvicted persons, the report asked “[A]re we citizens or suspects?” Considering that the NDNAD essentially creates a subset of people who are continuously under suspicion, despite potentially having never been convicted of any offense, GeneWatch U.K. argues that this may serve to “subtly alter” the way in which these people are viewed by their government or even by other citizens.<sup>134</sup>

In response to the argument that only the guilty have anything to fear, the GeneWatch U.K. report made reference to historical accounts of the misuse of citizen information by communist and fascist regimes throughout Europe.<sup>135</sup> GeneWatch U.K. reasoned that the fact there was no indication of wrongdoing was not a good enough argument for the expansion of the database; the potential for wrongdoing was enough.<sup>136</sup> Furthermore, the “nothing to hide” argument proceeds on the premise that valuing privacy is about hiding a wrong. While privacy is a difficult, perhaps impossible, notion to succinctly define, it encompasses such a range of ideas that it is safe to say that a desire for privacy does not necessarily stem from a guilty

---

<sup>126</sup> *Id.*

<sup>127</sup> *Id.*

<sup>128</sup> See GENEWATCH UK, *supra* note 18.

<sup>129</sup> *Id.* at 32.

<sup>130</sup> *Id.* at 36 (“[f]unction creep” refers to any potential future use of the databanks for purposes other than the investigation of criminal activity).

<sup>131</sup> *Id.* at 42.

<sup>132</sup> *Id.* at 12.

<sup>133</sup> *Id.* at 47.

<sup>134</sup> *Id.* at 29 (citations omitted).

<sup>135</sup> *Id.*

<sup>136</sup> *Id.*

conscience. The “nothing to hide” argument, while strong on its face, crumbles under scrutiny.

The GeneWatch U.K. report also indicated ways in which DNA profiles might be misused in the future. Specifically, it cited the possibility of attempts to use DNA sequences to predict ethnicity and using current NDNAD profiles to determine where a suspect may come from.<sup>137</sup> Depending on how a person views DNA sampling and retention, this could be considered either a powerful investigative tool or another way in which racial discrimination could be (and, in the view of some, is being) perpetuated.<sup>138</sup>

Additionally, the GeneWatch U.K. report included some statistics on what happens once someone is arrested by the police. While the survey was outdated, having taken place in 1993–1994, the results shed light on the implications of a DNA database as widely used as the NDNAD.<sup>139</sup> In that time frame, 1.75 million people had been arrested for both recordable and non-recordable offences.<sup>140</sup> Over one third of the arrestees had been detained for “relatively minor public order offenses” and only four percent had been arrested for the “most serious violent crimes.”<sup>141</sup> Of those arrested, only forty percent were eventually convicted.<sup>142</sup> Thus, of the persons arrested during that two-year period, over one million were never convicted.<sup>143</sup> Perhaps even more importantly, only fifty-two percent of suspects were even charged. The rest of the arrested persons either had no further action taken against them, were cautioned and released, or their charges were dealt with in “various other ways.”<sup>144</sup>

In 2006, Prime Minister Tony Blair indicated his support for a national DNA database, saying it was “vital for catching serious criminals.”<sup>145</sup> Echoing these sentiments in 2007, Lord Justice Sedley espoused his belief that the NDNAD should be expanded to include the DNA profile of every citizen in the U.K. in order to avoid discrimination against ethnic

---

<sup>137</sup> *Id.* at 31.

<sup>138</sup> *Id.* at 49.

<sup>139</sup> *Id.* at 41.

<sup>140</sup> *Id.*

<sup>141</sup> *Id.*

<sup>142</sup> *Id.*

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> George Jones, *DNA Database ‘Should Include All,’* TELEGRAPH (Oct. 24, 2006), <http://www.telegraph.co.uk/news/uknews/1532210/DNA-database-should-include-all.html>.

minorities.<sup>146</sup> Both men were met with resistance in Parliament from both the Liberal Democrats and the Conservatives and the database was never expanded that far.<sup>147</sup>

In 2007, the Nuffield Council on Bioethics issued a report (the Nuffield Report) strongly advocating against the government's then-current proposals for further expanding the power to take DNA samples.<sup>148</sup> The Nuffield Report advanced arguments regarding proportionality, costs of the system, and addressed the commonly advanced argument that "those who are innocent have nothing to fear."<sup>149</sup> Their response was even more concrete than that posited in the GeneWatch U.K. report. In addition to the "what if?" response indicated in GeneWatch, the Nuffield Report referenced the actual harm that can be suffered by an individual who is merely the subject of police suspicions.<sup>150</sup> Even without an arrest or investigation leading to a conviction, persons involved in a police investigation may be distressed throughout the process and stigmatized in society by mere association with a criminal investigation.<sup>151</sup>

Second, the Nuffield Report indicated that maintenance of the national database could actually hinder the pursuit of criminal justice. As a practical issue, the Nuffield Report noted that "fewer than 20% of crime scenes" actually undergo any type of forensic examination<sup>152</sup> and recommended that instead of increased sampling and retention of DNA, resources should be focused on fully examining crime scenes and other types of investigative work.<sup>153</sup> Further, the report claimed that a national DNA database, as advocated by some, would not only be hugely expensive, but it would in fact have a very small effect on national crime rates.<sup>154</sup> Despite claims that the collection and retention of DNA samples aids the prevention of crime, the crime rates in the U.K. have not shown a marked improvement.<sup>155</sup>

Third, the Nuffield Report warned that DNA evidence used during court proceedings sways juries a great deal, even though it may utilize science and

---

<sup>146</sup> *All UK 'Must be on DNA Database,'* BBC NEWS (Sept. 5, 2007), <http://news.bbc.co.uk/2/hi/uk/6979138.stm>.

<sup>147</sup> *New Police Powers Unveiled*, *supra* note 115.

<sup>148</sup> Michael Zander, *DNA: Time to Follow Scotland's Lead?*, 157 NEW L.J. 1446 (2007).

<sup>149</sup> NUFFIELD REPORT, *supra* note 121, at 33.

<sup>150</sup> *Id.* at 39–74; *see also* Zander, *supra* note 148.

<sup>151</sup> NUFFIELD REPORT, *supra* note 121, at 39–74.

<sup>152</sup> *Id.* at 47.

<sup>153</sup> *Id.* at 49.

<sup>154</sup> *Id.* at 54.

<sup>155</sup> *Id.*

statistics that jurors do not actually understand.<sup>156</sup> Like several other detractors, the Nuffield Report noted that the NDNAD could further exasperate problems with governance and ethical oversight, dangers of inferring ethnicity, and racial discrimination in criminal justice systems that already experience an ingrained type of discrimination.<sup>157</sup>

Fourth, the report showed concern over the fact that, in the U.K., children were treated the same as adults for the purposes of the NDNAD.<sup>158</sup> In 2005 there were roughly 740,000 persons in the database whose samples were obtained when they were under the age of eighteen.<sup>159</sup> Traditionally, criminal justice systems are more lenient on minors and treat them as equals to adults in only a handful of situations, often decided on a case-by-case basis. Thus, the inclusion of minors in the database in the same manner as adult records are obtained and kept is troubling.

Finally, with respect to volunteer samples and samples that were given with consent of the donating party, the Nuffield Council recommended that they not be held indefinitely; instead, the consent should be conditional and revocable.<sup>160</sup> Individuals who had provided samples in order to aid a specific criminal investigation should be able to condition the retention of their profiles on the duration of the investigation for which the sample was given.<sup>161</sup> Allowing this would permit those citizens to remove themselves from the pool of potential suspects, rather than treating volunteers the same as arrestees and convicts.

In light of the many issues identified, the final recommendation of the Nuffield Report was that police should only be allowed to retain the DNA information about persons who were convicted of a crime.<sup>162</sup> It noted in particular that the police power with regards to collecting and retaining DNA samples and other types of personal information was already comparatively broad in England and Wales.<sup>163</sup> Prior to the final recommendation of the U.K. government to further expand those powers, the Nuffield Report strongly advocated abandoning proposals that would allow for the collection

---

<sup>156</sup> *Id.* at 67.

<sup>157</sup> *Id.* at 77–84.

<sup>158</sup> *Id.* at 58–59.

<sup>159</sup> *Id.* at 58.

<sup>160</sup> *Id.* at 56.

<sup>161</sup> *Id.* at 54.

<sup>162</sup> *Id.*

<sup>163</sup> *Id.*

and retention of DNA samples for something as simple as littering and minor traffic offenses.<sup>164</sup>

Instead, the authors of the Nuffield Report indicated that the Scottish practices regarding DNA were a preferable alternative.<sup>165</sup> In Scotland (which was not affected by some of the legislation expanding the retention of samples and profiles in the NDNAD),<sup>166</sup> only the samples of those “charged with serious violent or sexual offences” could be retained without a conviction.<sup>167</sup> Even then, the samples could only be kept for three to five years.<sup>168</sup> Profiles and samples taken in connection with other recordable offences would require a conviction in order to be maintained in the databank.<sup>169</sup> It is in the face of these growing concerns and arguments against the widespread use of the NDNAD, and with extraordinary technological advances being made in the field of DNA identification, that the European Court for Human Rights heard the pivotal case of *S. & Marper v. United Kingdom*.

#### IV. THE EUROPEAN COURT OF HUMAN RIGHTS’ DECISION IN *S & MARPER V. UNITED KINGDOM*

*S. & Marper v. United Kingdom* was the critical case in which the ECtHR ruled that the indefinite retention of DNA profiles from persons arrested but never convicted of a crime constituted violations of the Convention.<sup>170</sup> In each of their cases, both S. (name excluded because he was a minor at the time of arrest) and Marper had been arrested but never convicted.<sup>171</sup> S. had been arrested at the age of eleven for robbery, and Marper was arrested for harassment of his partner.<sup>172</sup> S. was acquitted of the charges against him and the case against Marper was discontinued.<sup>173</sup>

Each defendant petitioned the police to have their DNA samples and fingerprints destroyed, but these requests were refused.<sup>174</sup> When they took

---

<sup>164</sup> *Id.* at 10, 44.

<sup>165</sup> *Id.* at 54.

<sup>166</sup> *See supra* Part II.C.

<sup>167</sup> NUFFIELD REPORT, *supra* note 121, at 54.

<sup>168</sup> *Id.*

<sup>169</sup> *Id.*

<sup>170</sup> *S. & Marper v. United Kingdom*, [2008] Eur. Ct. H.R. 1581.

<sup>171</sup> *Id.* at 10–11.

<sup>172</sup> *Id.*

<sup>173</sup> *Id.* at 11.

<sup>174</sup> *Id.* at 12.



their respective challenges to the Administrative Court, S. and Marper were rejected there as well.<sup>175</sup> The Court of Appeal, in upholding the decision of the Administrative Court, determined that “DNA *profiles* reveal only limited personal information.”<sup>176</sup>

The ECtHR began its opinion by noting that “privacy” had never been exhaustively defined in English law.<sup>177</sup> The court determined, therefore, that privacy can include multiple elements of one’s identity, including health information and ethnicity.<sup>178</sup> It further found, unequivocally, that all three categories of information at question in the case (fingerprints, DNA profiles, and cellular samples) are personal data such that they fall within the purview of the Data Protection Act 1998.<sup>179</sup>

Further, in holding that the indefinite retention of DNA samples of unconvicted persons constituted a violation of the Human Rights Act, the court found that DNA samples contain a “substantial amount” of personal data, particularly considering the ability to identify the possible perpetrator of a crime from examining the DNA of his family members.<sup>180</sup> The ECtHR determined that the retention of these samples interfered with the petitioners’ rights to a private life.<sup>181</sup> The court also noted that the U.K. was the only member state of the Council of Europe that expressly permitted the indefinite retention of DNA and cellular samples of people who had never been convicted of a crime.<sup>182</sup>

Depending heavily on its opinion in *Van der Velden v. the Netherlands*, the court focused on how the information contested in this case might be used, or misused, in the future.<sup>183</sup> *Van der Velden* concerned cellular material; there, the court considered that, “given the use to which cellular material in particular could conceivably be put in the future, the systematic retention of that material was sufficiently intrusive to disclose interference with the right to respect for private life.”<sup>184</sup>

The ECtHR further held in *Marper* that the indefinite retention of personal information contained in cellular samples constitutes a per se

---

<sup>175</sup> *Id.*

<sup>176</sup> *Id.* at 13 (emphasis in original).

<sup>177</sup> *Id.* at 66.

<sup>178</sup> *Id.*

<sup>179</sup> *Id.* at 68.

<sup>180</sup> *Id.* at 75.

<sup>181</sup> *Id.* at 77.

<sup>182</sup> *Id.* at 110.

<sup>183</sup> *Id.* at 19.

<sup>184</sup> *Id.* at 70 (citing *Van der Velden v. Neth.*, 1174 Eur. Ct. H.R. (2006)).

interference with the right to respect for a private life.<sup>185</sup> The fact that authorities only use a limited portion of the information contained in those samples was of no consequence to the Court's ruling.<sup>186</sup> Even considering the difference between samples and profiles, the court noted that DNA profiles "contain substantial amounts of unique personal data" that go far beyond only providing information about identity.<sup>187</sup> As support for this proposition, the Court noted the ability of a DNA profile to identify familial relationships or ethnic origin.<sup>188</sup>

In 2010, in the aftermath of the ECtHR's ruling, the U.K. changed the law to specify that acquitted citizens' DNA profiles collected during an investigation of a crime may only be retained for a maximum of six years.<sup>189</sup> While some commentators argue that the new incarnation is still a violation of the HRA,<sup>190</sup> it has yet to be overruled. Additionally, even though the DNA records of unconvicted persons were removed from the system, records of arrest remain and the law allows these arrest records to remain accessible indefinitely.<sup>191</sup>

#### V. THE SUPREME COURT OF THE UNITED STATES' DECISION IN *MARYLAND V. KING*

The case of *Maryland v. King* involves petitioner Alonzo King who was arrested in 2009 on assault charges.<sup>192</sup> Upon arrest, King underwent a buccal swab for collection of his DNA as part of routine booking procedure in Maryland.<sup>193</sup> His DNA was linked to a rape that had occurred in 2003 and he was convicted on those charges.<sup>194</sup> King challenged this conviction on the

---

<sup>185</sup> *Id.* at 73.

<sup>186</sup> *Id.*

<sup>187</sup> *Id.* at 75.

<sup>188</sup> *Id.* at 75–76.

<sup>189</sup> Keith Soothill, *Public/Human Rights: The Debate Rumbles On*, 160 NEW L.J. 94 (2010).

<sup>190</sup> Laura McGowan, *Criminal Law Legislation Update*, 3 J. CRIM. L. 284, 288 (2009).

<sup>191</sup> As of April 2009, the arrest records of 986,185 people who had never been convicted, reprimanded, or in any other way cautioned remained in the Police National Computer (PNC). These records are not only accessible by law enforcement agencies but also by prospective employers who choose to do an "enhanced" criminal records check, with potentially job-limiting implications. Jamie Doward, *Names of Innocent People Will Stay on Police Database*, OBSERVER, Dec. 19, 2009, <http://www.theguardian.com/politics/2009/dec/20/dna-police-database.rights>.

<sup>192</sup> *Maryland v. King*, 133 S. Ct. 1958 (2013).

<sup>193</sup> *Id.* at 1965.

<sup>194</sup> *Id.*

basis that the collection of his DNA incident to his arrest for assault was an unreasonable search and seizure.<sup>195</sup> The Supreme Court upheld his conviction, finding the search reasonable under the Fourth Amendment. In doing so, it may have taken the first step towards more comprehensive DNA collection and retention laws, allowing the United States to follow the footsteps of the United Kingdom into a mire of privacy violations.

The Maryland statute on DNA collection (the Act) provides for the collection of DNA from arrestees who are charged with violent crimes, burglary, attempted violent crimes, and attempted burglary.<sup>196</sup> Once the sample is collected, it may only be uploaded to a database after the accused has been arraigned.<sup>197</sup> The Act does contain a number of safeguards. For instance, it allows for the immediate destruction of any samples if the accused is acquitted, the conviction is reversed, or the defendant is pardoned.<sup>198</sup>

The Supreme Court, in its majority opinion, mentioned each of the aforementioned safeguards. However, the Court never indicated which of these safeguards, if any, were essential to its holding that a search and seizure pursuant to the Act constituted a reasonable invasion of privacy given the state interests to be served.<sup>199</sup> The state interests advanced by the *King* Court strongly resemble some of those advanced by advocates of the NDNAD in the U.K., including: identification of potential criminals, ensuring the safety of those charged with detaining arrestees, ensuring the presence of the accused at trial, assessing the danger a person may pose to the public at large, and freeing the wrongfully accused.<sup>200</sup> These are strong state interests and the use of DNA in criminal investigations in furtherance of these interests is indisputable. However, the Court focused heavily on these end goals, noting the “unmatched potential of DNA identification”<sup>201</sup> to serve them, but glossed lightly over the privacy interests at stake.

There are two prongs to assessing the reasonableness of a search: the level of invasion or intrusiveness of the search and the person’s legitimate expectations of privacy.<sup>202</sup> Beginning with the level of intrusion necessary to

---

<sup>195</sup> *Id.*

<sup>196</sup> MD. CODE ANN., PUB. SAF. § 2-504(a)(3)(i).

<sup>197</sup> *Id.* § 2-504(d)(1).

<sup>198</sup> *Id.* § 2-511(a)(1).

<sup>199</sup> *King*, 133 S. Ct. at 1979–80.

<sup>200</sup> *Id.* at 1971–74.

<sup>201</sup> *Id.* at 1977.

<sup>202</sup> *Id.* at 1977–79.

obtain a DNA sample, Justice Kennedy assures the reader that a buccal swab is a minimal intrusion; a simple swipe of the cheek is in no way comparable to invasive surgery, or even as invasive as some other normal booking procedures.<sup>203</sup> Next, the opinion addresses the arrestee's "legitimate expectations of privacy." It is well-settled that persons who undergo an arrest supported by probable cause have a reduced expectation of privacy.<sup>204</sup> The opinion indicates that the sampling of one's DNA is not as invasive or potentially revealing as a search of one's home.<sup>205</sup> However, this view is flawed.

The Court in this case focuses on the importance of DNA profiles for the identification of an accused. In its review of the amount of information contained in a DNA profile, the opinion glosses over the ability to determine ethnic origin or familial relationships.<sup>206</sup> It compares a DNA profile to a photograph or a fingerprint,<sup>207</sup> both of which are capable of revealing much less information about a person than is a DNA profile. The Court thus frames DNA profiles as nearly harmless intrusions upon a person who has a diminished expectation of privacy because they have already been suspected of some sort of wrongdoing.

In his blistering dissent, joined by Justices Kagan, Ginsburg, and Sotomayor, Justice Scalia heavily criticizes the majority opinion's reliance on the fact that DNA is used only for identification.<sup>208</sup> He notes that fingerprints and photographs are taken for purposes of identification; DNA is taken for purposes of solving crimes.<sup>209</sup> He appreciates that this is a noble objective, but argues that it must fall to other more important goals, including protecting citizens from suspicionless searches.<sup>210</sup> Justice Scalia's premonition is simple: "As an entirely predictable consequence of [this] decision, your DNA can be taken and entered into a national DNA database if you are ever arrested, rightly or wrongly, and for whatever reason."<sup>211</sup>

---

<sup>203</sup> *Id.* at 1976–79.

<sup>204</sup> *Id.* at 1978.

<sup>205</sup> *Id.* at 1979 ("Some searches, such as invasive surgery, or a search of the arrestee's home, involve greater intrusions or higher expectations of privacy than are present in this case." (citations omitted)).

<sup>206</sup> *Id.* at 1972.

<sup>207</sup> *Id.*

<sup>208</sup> *Id.* at 1958 (Scalia, J., dissenting).

<sup>209</sup> *Id.* at 1987.

<sup>210</sup> *Id.* at 1989.

<sup>211</sup> *Id.*

Thus, a likely long-term consequence of this opinion will be a U.S. equivalent to the NDNAD.

Bolstering this conclusion is the apparent breadth of the decision itself. The majority in this case notes that its decision will implicate the DNA collection statutes in every state that has such legislation, yet it issues a broad opinion that offers little guidance to state legislatures or lower courts. By treating DNA as a simple identification tool, the Court simply puts off the decision of what limits there must be to DNA collection, retention, or use. More importantly, without noting which of the safeguards found in the Maryland Act are essential to the legitimate protection of privacy, the Court opens the door for a multitude of DNA collection and retention statutes that range in their levels of protection. In stressing the importance of the state interests to be served and diminishing the far-reaching capabilities of forensic DNA analysis, the Court has opened the door for the U.S. to legislate itself into the same predicament that the U.K. was in by 2008.

## VI. CONCLUSION

In the early days of using DNA as an investigative tool, governments were optimistic about the ability of this new technology to help solve and potentially prevent crime. It was, and remains, one of the most powerful tools available to those involved with criminal investigations. In the U.K., this optimism, combined with public approval and a lack of a clearly defined right to privacy, enabled the creation and evolution of one of the largest and fastest growing DNA databases in the world. Over the course of a decade, the U.K. continuously passed legislation that expanded its police power in an unprecedented fashion.

As the U.K. government became more industrious in its cataloguing of personal information, the public and various human rights groups became concerned with the system's potential to violate personal privacy rights. Eventually, the ECtHR held that the U.K. had surpassed its limits and ruled that the indefinite retention of DNA samples and profiles from unconvicted persons was a violation of international human rights law.

The ECtHR hinged its decision on the unlimited time span for which personal information could be retained by the government, the nature of the information that could be gleaned from a DNA sample or profile, and the difficulties innocent people face in getting their records erased from the national database. As a direct result of this ruling, profiles of unconvicted

persons are no longer allowed to remain in the U.K. databases indefinitely, irrespective of the claimed governmental interest in preventing crime.

While the U.K. is different from some democratic societies in that it has no statutory or constitutional right to privacy, other countries may be well served by considering the evolution of laws regarding DNA databases in the U.K., as well as the ruling and reasoning of the ECtHR in *Marper*, in fashioning their own arrestee DNA legislation or databases. In the United States, of the twenty-eight states that allow for the collection of DNA upon arrest, only seven also require state-initiated expungement; the rest specify that it is the citizen's responsibility to initiate expungement proceedings.<sup>212</sup>

Requiring citizen-initiated expungement can be problematic for many reasons, such as the time involved in obtaining a court order and socioeconomic factors that may disproportionately prevent one class of people from navigating the legal system in an attempt to get a court order, among others. Considering the additional required time and costs of obtaining a lawyer to assist with procuring the necessary order for expungement, most citizens are unlikely to go through the process necessary to have their DNA profile removed from the databases. This, in turn, translates to more and more profiles of exonerated or acquitted persons being retained in the DNA databases—the exact practice the ECtHR took steps to eliminate.

As the United States strives toward using DNA technology to its full advantage without violating the rights of citizens, it may be useful to consider the findings of other high courts, as well as the overall evolution of DNA legislation in other countries. The Supreme Court's opinion in *Maryland v. King* found that a simple buccal swab to obtain a DNA sample for the purposes of identification of a person arrested for a serious offense was not an unreasonable search under the Fourth Amendment. While the Maryland law in question in *King* had many of the safeguards desired by privacy rights advocates and mentioned by the ECtHR, the Court's decision was not expressly limited to those statutes with similar protective measures. Furthermore, the U.S. Supreme Court views DNA profiles primarily as a mode of identification, and it did not concern itself with future potential uses or the potential for familial searches. Many would argue that this is an oversimplification of the true utility of DNA profiles and databases, but that is an argument that the Court is sure to see again. It is highly likely that DNA collection statutes will continue to proliferate in the United States, and

---

<sup>212</sup> See Samuels et al., *supra* note 1, at 19–23.

the Court will face challenges to the scope of such statutes in the future. While the decision in *Maryland v. King* may be reminiscent of the strong support DNA collection and retention initially enjoyed in the U.K., it remains to be seen if the United States will allow the establishment of a system as far-reaching and comprehensive as the NDNAD.

An individual's right to privacy and right to be free from unnecessary government interference—the “right to be let alone—are core values not only of the American legal system, but also of American culture.<sup>213</sup> In this country and in any other country considering arrestee DNA sampling and retention, legislation should always be considered in light of the statistics surrounding arrestee DNA sampling, the potentially inadequate safeguards against sample retention in cases that result in nonconviction, and the difficulties many would face in getting their records expunged if the process is not state-initiated. Otherwise, arrestee DNA databases across the world may experience a fate similar to that of the NDNAD in the U.K.—continuously strengthened until the system infringes on any number of human rights.

---

<sup>213</sup> *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (“[T]he right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men.”).