

2011

The Double-Helix Double-Edged Sword: Comparing DNA Retention Policies of the United States and the United Kingdom

Erica S. Deray

Follow this and additional works at: <https://scholarship.law.vanderbilt.edu/vjtl>



Part of the [Human Rights Law Commons](#), [Law Enforcement and Corrections Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Erica S. Deray, The Double-Helix Double-Edged Sword: Comparing DNA Retention Policies of the United States and the United Kingdom, 44 *Vanderbilt Law Review* 745 (2021)
Available at: <https://scholarship.law.vanderbilt.edu/vjtl/vol44/iss3/5>

This Note is brought to you for free and open access by Scholarship@Vanderbilt Law. It has been accepted for inclusion in Vanderbilt Journal of Transnational Law by an authorized editor of Scholarship@Vanderbilt Law. For more information, please contact mark.j.williams@vanderbilt.edu.

The Double-Helix Double-Edged Sword: Comparing DNA Retention Policies of the United States and the United Kingdom

ABSTRACT

Forensic scientists have used DNA profiling technologies to link suspects to crimes since Alec Jeffreys first proposed the idea in the 1970s. Recognizing the potential for using DNA databases to solve crimes and to prevent future crimes, England and Wales attempted to greatly expand its DNA database by allowing for the collection and indefinite retention of DNA profiles from arrestees. The European Court of Human Rights, however, issued a ruling in 2008 in the case of S. & Marper v. United Kingdom, advising the United Kingdom to restrict use of DNA profiles from arrestees and to establish time frames for removal of this information from databases. Conversely, in the United States, federal and state legislation have become increasingly expansive and many states and the federal government now allow for collection of DNA samples from arrestees. This Note considers the evolving United States laws governing DNA databases in light of the Marper decision and proposes placing limits on the ability of law enforcement to use and retain DNA profiles from arrestees.

TABLE OF CONTENTS

I.	INTRODUCTION	746
II.	BACKGROUND	748
A.	<i>An Overview of DNA Technology</i>	748
B.	<i>The United Kingdom</i>	750
	1. History of Forensics in the United Kingdom	750
	2. <i>The S. & Marper v. the United Kingdom Decision</i>	754
	3. Responses to <i>Marper</i> : Changing Approaches to DNA Retention	754
C.	<i>The United States and Forensic Science Legislation</i>	755
	1. History of DNA in the United States.....	755

	2. Judicial Decision-Making Regarding	
	DNA	759
	D. <i>Alternative DNA Collection Practices</i>	761
III.	ANALYSIS	763
	A. <i>Privacy Concerns</i>	764
	B. <i>Innocent Until Proven Guilty</i>	766
	C. <i>The Implications of Indefinite Retention of</i> <i>DNA Profiles</i>	768
IV.	SOLUTION	772
V.	CONCLUSION	774

It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of his presence.

—Edmond Locard¹

I. INTRODUCTION

Criminal investigations have increasingly come to rely on the use of technology and scientific advancements to identify suspects and solve crimes.² At the center of this movement is the use of DNA profiling to link suspects with crimes and to exonerate convicted individuals by excluding them as possible sources of DNA collected from crime scenes.³ DNA collection from individuals in the criminal context occurs under essentially one of four possible policies: (1) collection of DNA only from individuals who are charged and convicted of crimes; (2) DNA collection from arrestees with indefinite retention of DNA profiles on a database; (3) DNA collection from arrestees with removal of DNA profiles upon request; and (4) DNA collection from arrestees with automatic expungement.

England is at the forefront of the movement to use DNA to solve crimes, and the England and Wales National DNA Database is the largest forensic database in the world.⁴ Recognizing the potential for using DNA to solve crimes and to prevent future crimes, England attempted to greatly expand its DNA database by allowing for the

1. LEROY LAD PANEK, *THE ORIGINS OF THE AMERICAN DETECTIVE STORY* 168 (translating EDMOND LOCARD, *MANUEL DE TECHNIQUE POLICIÈRE* (1923)).

2. See LAWRENCE KOBILINSKY ET AL., *DNA: FORENSIC AND LEGAL APPLICATIONS 1-7* (2005) (describing the “evolution of identification” in criminal investigations).

3. *Id.* at 5-7.

4. Rowena E. Rodrigues, *Big Bio-Brother Is Here: Wanting, Taking and Keeping Your DNA 2* (British & Irish Law, Educ. & Tech. Ass’n, 2007), <http://www.bileta.ac.uk/Document%20Library/1/Big%20Bio-Brother%20is%20here%20-%20wanting,%20taking%20and%20keeping%20your%20DNA.pdf>.

collection and indefinite retention of DNA profiles from arrestees.⁵ Collecting and retaining DNA from individuals who were not convicted of a crime raises concerns about the privacy interests of the individual versus possible benefits to society.⁶ Similar concerns are present when legislation allows for the indefinite retention of samples from convicted persons. Even Alec Jeffreys, whose discoveries revolutionized the use of DNA in criminal cases, expressed concern about the selective expansion of DNA databases.⁷ He commented that retaining suspects' DNA is "likely to be discriminatory; it won't affect people at random but be skewed in favour of certain socioeconomic and ethnic groups."⁸

The United States has begun to move toward a system similar to that present in the United Kingdom prior to the *S. & Marper* decision. Federal legislation now allows for the collection of DNA samples from arrestees.⁹ Additionally, a number of states have passed similar legislation, and both state and federal courts have ruled that these laws are constitutional.

This Note examines the implications of the emerging trend in the United States toward looser restrictions on DNA retention and collection, and proposes that federal and state legislatures act now to prevent future abuses in the use of expanded DNA databases. Part II provides an overview of the use of forensic DNA analysis and the ways in which the technology has developed to facilitate law enforcement's efforts to solve both new and previously unsolved crimes. It then examines the current system in the United Kingdom and evolving trends in United States DNA collection and retention. Part III compares the DNA profiling system in the United Kingdom following the *Marper* decision with the current system in the United States. It also analyzes the potential risks that are present if the United States continues with its current trend toward permitting collection and retention of DNA from arrestees. Part IV proposes to restrict the ability of law enforcement to retain DNA profiles collected from arrestees. It further establishes guidelines barring the use of forensic technology to conduct familial searches on DNA profiles, unless permission has been given by the source of the original profile or in certain exceptional circumstances.

5. *S. & Marper v. United Kingdom*, 2008 Eur. Ct. H.R. 1581, ¶¶ 45–47.

6. See *infra* Part III.A (discussing the privacy interests of individuals from whom DNA may be collected).

7. See Frances Gibb, *The DNA Scientist Who Made Individuals of Us All*, *Times*, Dec. 6, 2005, <http://business.timesonline.co.uk/tol/business/law/article745719.ece> (discussing Jeffreys's concerns that retaining suspects' DNA may affect certain socioeconomic and ethnic groups more than others and may inappropriately disclose information about familial relationships).

8. *Id.*

9. See *infra* notes 95–97 and accompanying text (discussing federal legislation governing DNA collection).

II. BACKGROUND

A. An Overview of DNA Technology

Physical evidence has long helped law enforcement to solve crimes.¹⁰ Given the unreliability, and sometimes unavailability, of eyewitnesses, physical evidence may be the only means of solving a crime.¹¹ Physical evidence can range from something as seemingly simple as a shoeprint¹² to something as complex as DNA. The use of fingerprints and blood typing was a precursor to DNA sampling,¹³ and law enforcement began classifying, storing, and retrieving fingerprint data using computers in the early 1970s.¹⁴ Fingerprints are often said to provide “absolute proof of identity,” because they remain the same throughout a person’s lifetime and are unique to each individual.¹⁵ DNA profiling has now emerged as a method of identifying the source of biological evidence that rivals fingerprint analysis in reliability and effectiveness.¹⁶

In the early 1980s, two fifteen-year-old girls were raped and murdered in a village in England.¹⁷ The crimes occurred three years apart, but no arrest could be made until after the second murder.¹⁸ Despite receiving a confession from one man for the second crime, law enforcement was able to use DNA forensic techniques to determine that the same man had murdered both girls, and it was not the man who had confessed.¹⁹ In making this discovery, police received cooperation from approximately five thousand local men who volunteered to have DNA samples collected and tested.²⁰ Colin

10. See KOBILINSKY ET AL., *supra* note 2, at 1–7 (describing different types of physical evidence and their use in criminal investigations).

11. *Id.* at 1.

12. See *id.* at 1–2 (describing how crime scene investigators utilize shoe prints as evidence).

13. See Frederick R. Bieber, *Science and Technology of Forensic DNA Profiling: Current Use and Future Directions*, in *DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE* 23, 24–25 (David Lazer ed., 2004) (discussing the origins of forensic identity testing, including the use of fingerprint ridge pattern analysis and identification of heritable variations in human blood types).

14. KOBILINSKY ET AL., *supra* note 2, at 5.

15. *Id.* at 3–4.

16. *Id.* at 5; see also MALCOLM DAVIES ET AL., *CRIMINAL JUSTICE: AN INTRODUCTION TO THE CRIMINAL JUSTICE SYSTEM IN ENGLAND AND WALES* 97 (1995) (“The use of DNA profiling was also regarded as reliable as fingerprinting to check the unique characteristics of an individual.”).

17. Gibb, *supra* note 7.

18. *Id.*

19. *Id.*

20. *Id.*

Pitchfork eventually came forward and police were able to match his DNA to both crimes in the first successful use of such technology.²¹

DNA is the genetic material that is partially responsible for transmitting individual characteristics from parents to offspring.²² In the mid-1970s, laboratory methods were developed to detect genetic variation at the DNA level.²³ While some portions of DNA do not differ between individuals,²⁴ there is enough variation in 2 percent of the genome to make DNA sequencing and the creation of DNA profiles useful in forensic analysis.²⁵ Different methods were developed and utilized for forensic DNA analysis,²⁶ but the need to have DNA that is of both sufficient quality and quantity continues to limit their use.²⁷ Some advances, such as the polymerase chain reaction (PCR) DNA typing procedure, now allow criminalists to replicate DNA, thereby expanding its usability.²⁸ In order for DNA evidence to be useful, it remains particularly important to maintain the integrity of the DNA samples collected.²⁹ Problems that can arise during the analysis procedure include contamination, degradation, interference from environmental conditions, the presence of inhibitors, and human error.³⁰

DNA profiles extracted from the evidence are then compared to DNA found in blood or tissue taken from known samples, and one of these interpretations usually applies: inclusion, exclusion, or inconclusive.³¹ A finding of inclusion indicates that there was a match between a known sample and the evidentiary sample.³² If an interpretation of DNA inclusion is made, testifying experts must provide fact-finders, such as jurors, with estimates of the likelihood of finding the particular DNA profile in a randomly selected individual and with statistics about how rare the profile is in the relevant

21. *Id.*; see also Gary Cordner & Kathryn E. Scarborough, *The Myth that Science Solves Crimes*, in DEMYSTIFYING CRIME AND CRIMINAL JUSTICE 104, 107–08 (Robert M. Bohm & Jeffery T. Walker eds., 2006) (describing the use of DNA by law enforcement in the United States and the United Kingdom).

22. Bieber, *supra* note 13, at 25.

23. *Id.*

24. KOBILINSKY ET AL., *supra* note 2, at 6.

25. Bieber, *supra* note 13, at 26.

26. See *id.* at 28–34 (discussing laboratory procedures, including the use of the polymerase chain reaction).

27. See KOBILINSKY ET AL., *supra* note 2, at 19 (“Thus, insufficient quantity and poor quality of the sample often limited the ability to obtain useful identifying information.”).

28. *Id.* at 19, 71.

29. See *id.* at 28–34 (describing procedures for packaging and preserving biological evidence found at a crime scene).

30. See *id.* at 129–34 (describing further how these factors can interfere with the analysis of biological evidence).

31. Bieber, *supra* note 13, at 34–35.

32. *Id.* at 35.

population.³³ In the United States, the major population groups include Caucasians, Blacks, West Coast Hispanics, East Coast Hispanics, and Asians.³⁴

Previously, prosecutors and laboratories had to be cognizant of the fact that findings were of little or no statistical significance if the database size was too small.³⁵ As the technology has evolved and databases have increased in size, however, juries are often told that a particular “genetic profile is as rare as one in a trillion . . . [and] is essentially an absolute identification.”³⁶ With jurors becoming increasingly confident in and reliant upon these DNA testing results, laboratories must exercise proper quality control and quality assurance procedures to avoid the potentially tragic consequences of a false exclusion or inclusion.³⁷

B. *The United Kingdom*

1. History of Forensics in the United Kingdom

Britain was the first country to have a national DNA database.³⁸ The Royal Commission on Criminal Justice³⁹ recommended the establishment of the DNA database in 1993,⁴⁰ and the Home Office officially announced its creation a year later.⁴¹ At that time, the Home Office also commissioned a pilot study to examine the use of DNA in the context of a forensic database.⁴² In 1995, the Criminal Justice and Public Order Act (CJPOA) mandated establishment of the England and Wales National DNA Database (NDNAD), and it has since become the largest forensic database in the world.⁴³ The NDNAD is maintained by the Forensic Science Service (FSS) in Birmingham.⁴⁴ The FSS, a quasi-governmental agency, also performs 90 percent of England’s forensic DNA analysis.⁴⁵

33. KOBILINSKY ET AL., *supra* note 2, at 149; Bieber, *supra* note 12, at 35–36.

34. KOBILINSKY ET AL., *supra* note 2, at 149–50.

35. *Id.* at 126.

36. *Id.* at 157.

37. *See id.* (“Failure to perform the DNA tests properly could lead to false exclusions as well as false inclusions, sometimes with tragic consequences.”).

38. DAVIES ET AL., *supra* note 16, at 97.

39. The Royal Commission on Criminal Justice was established in 1991 in response to concerns about public confidence in the criminal justice system. CHRISTOPHER H. ASPLEN, THE APPLICATION OF DNA TECHNOLOGY IN ENGLAND AND WALES 4 (2004), <http://www.ncjrs.gov/pdffiles1/nij/grants/203971.pdf>.

40. *Id.*

41. DAVIES ET AL., *supra* note 16, at 97.

42. ASPLEN, *supra* note 39, at 5.

43. Rodrigues, *supra* note 4, at 2.

44. GRAEME LAURIE, GENETIC PRIVACY: A CHALLENGE TO MEDICO-LEGAL NORMS 91 n.29 (2002); *see also* Circular 16/95 from Peter Wrench, Head, Policing Organised Crime Unit, to the Chief Officer of Police of England and Wales (Mar. 31,

Prior to enactment of the CJPOA, collection of evidence from suspects was permitted pursuant to the 1984 Police and Criminal Evidence Act (PACE),⁴⁶ which required a “serious arrestable offence”⁴⁷ and only allowed police to collect fingerprints.⁴⁸ Additionally, an officer could only take fingerprints without consent in the following circumstances: if an officer of at least the rank of superintendent authorized the taking, if the person was charged with a recordable offense, or if the person was informed that he or she would be reported for such an offense.⁴⁹ Thus, the CJPOA expanded the scope of data that police could collect for the NDNAD to include intimate samples (e.g., blood or other similar samples from which police can collect DNA) and also expanded the scope of suspects from whom police could take samples to include those charged with any “recordable offense.”⁵⁰

PACE also originally indicated that the government would not maintain an individual’s profile in the database unless the arrest resulted in a conviction.⁵¹ However, administrative problems led to cases in which DNA samples were not expunged but instead were used to identify suspects.⁵² In order to take advantage of the database’s ability to help identify suspects without criminal records, the House of Lords expanded the law in 2001 to permit indefinite retention of samples from individuals who were arrested, even if the arrest did not ultimately result in a conviction.⁵³

Under PACE, suspects received a number of protections to govern their dealings with police, including requirements that police document all traffic stops and tape record interviews at police stations.⁵⁴ Furthermore, PACE established that police must have reasonable grounds to suspect that they will find a stolen or prohibited article prior to searching a person or a vehicle in a public

1995) (describing the legal foundation of the DNA database and providing guidance on its operational use).

45. ASPLEN, *supra* note 39, at 3–4.

46. PACE was introduced in the United Kingdom in an effort to inform and guide police powers to stop and search, and to arrest. DAVIES ET AL., *supra* note 16, at 101–05.

47. ASPLEN, *supra* note 39, at 5.

48. *See id.* at 5–6 (discussing the classification of intimate and non-intimate samples and the limitations in place on the collection of the former).

49. Police and Criminal Evidence Act, 1984, c. 60, § 61 (Eng.).

50. Criminal Justice and Public Order Act, 1994, c. 33, § 54 (Eng.); ASPLEN, *supra* note 39, at 5.

51. Police and Criminal Evidence Act § 64; ASPLEN, *supra* note 39, at 5.

52. ASPLEN, *supra* note 39, at 6.

53. Criminal Justice and Police Act, 2001, c. 16, § 82 (Eng.); ASPLEN, *supra* note 39, at 6; *see also* LAURIE, *supra* note 44, at 91–92 (discussing public support for expanding DNA retention under the Criminal Justice and Police Act of 2001).

54. DAVIES ET AL., *supra* note 16, at 101.

place.⁵⁵ The concept of reasonable grounds also extended to arrests, and §§ 24–33 of PACE authorized police to “arrest anyone who is, or whom they reasonably suspect to be, committing an arrestable offence, and anyone who has committed or who can reasonably be suspected of having committed an arrestable offence.”⁵⁶

In 2006, the Association of Chief Police Officers in England and Wales issued Retention Guidelines for Nominal Records on the Police National Computer (Retention Guidelines) to provide guidance regarding the varying degrees of access to fingerprint and DNA records. The Retention Guidelines distinguished between police and non-police agencies who share data with them, and access depended on a number of factors, including time elapsed since conviction, the seriousness of the offense, and the age of the suspect.⁵⁷ Data regarding individuals who were not convicted of an offense were not accessible to the non-police agencies.⁵⁸ Furthermore, when individual police officers requested a search be carried out in conjunction with DNA from a crime scene, they received only information about profiles that match the DNA sample and did not have access to the database itself.⁵⁹

In November 2008, the House of Lords approved an amendment to the Counter Terrorism Bill that established a process assisting innocent people in removing their DNA and fingerprints from the national database.⁶⁰ Baroness Hanham, who proposed the amendment, stated: “There is no transparency in the current situation and the dice are severely loaded against innocent people being able to ensure that their most personal details are not kept indefinitely following their exclusion”⁶¹ The Council of Europe has also provided a number of recommendations in effect in the United Kingdom that provide guidance for the use of personal data,

55. *Id.*

56. *Id.* at 103.

57. ASS'N OF CHIEF POLICE OFFICERS, RETENTION GUIDELINES FOR NOMINAL RECORDS ON THE POLICE NATIONAL COMPUTER ¶¶ 1.5–1.6 (2006), <http://www.acpo.police.uk/documents/PoliceCertificates/SubjectAccess/Retention%20of%20Records06.pdf>; see also *S. & Marper v. United Kingdom*, 2008 Eur. Ct. H.R. 1581, ¶¶ 33–34 (discussing the Retention Guidelines and noting that they “are based on a format of restricting access to the Police National Computer (PNC) data, rather than the deletion of that data”).

58. *Marper*, 2008 Eur. Ct. H.R. ¶ 34.

59. HOME OFFICE, KEEPING THE RIGHT PEOPLE ON THE DNA DATABASE: SCIENCE AND PUBLIC PROTECTION, ¶¶ 4.8–4.9 (2009), <http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/dna-consultation?view=Binary> [hereinafter HOME OFFICE CONSULTATION].

60. *Lords Votes in Favour of DNA-Deletion Process*, ZDNet UK (Nov. 6, 2008), <http://news.zdnet.co.uk/security/0,1000000189,39543009,00.htm>.

61. *Id.*

including DNA samples.⁶² The Council, in the “Explanatory Memorandum to Recommendation No. R(92)1 . . . [on] [t]he use of analysis of [DNA] within the framework of the criminal justice system,” noted that “[s]ince the primary aim of the collection of samples and the carrying out of DNA analysis on such samples is the identification of offenders and the exoneration of suspected persons, the data should be deleted once persons have been cleared of suspicion.”⁶³ Of the at least twenty Council of Europe member states that allow DNA information to be taken and stored, the United Kingdom was the only one to expressly permit the systematic and indefinite retention of DNA samples and profiles of individuals who were acquitted or against whom charges had been dropped.⁶⁴

The provisions that governed DNA retention in England and Wales were the same as those in force in Northern Ireland, but continued to be more permissive than those of other European countries.⁶⁵ In Scotland, for example, the 1995 Criminal Procedure Act of Scotland establishes specific requirements for when officials must destroy samples and the resulting profiles:

[T]he DNA samples and resulting profiles must be destroyed if the individual is not convicted or is granted an absolute discharge. A recent qualification provides that biological samples and profiles may be retained for three years, if the arrestee is suspected of certain sexual or violent offences even if a person is not convicted (section 83 of the 2006 Act, adding section 18A to the 1995 Act.). Thereafter, samples and information are required to be destroyed unless a Chief Constable applies to a Sheriff for a two-year extension.⁶⁶

This statute caused some to question whether England and Wales should formulate more restrictive policies, and the European Court of Human Rights ultimately decided a case that addressed DNA retention policies.

62. See *Marper*, 2008 Eur. Ct. H.R. ¶¶ 41–44 (describing Council of Europe texts); see also, e.g., *Recommendation No. R (92) 1 of the Committee of Ministers of Member States on the Use of Analysis of Deoxyribonucleic Acid (DNA) Within the Framework of the Criminal Justice System*, at 1 (Feb. 10, 1992), available at <https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2> (recommending how DNA samples should be used by law enforcement in member and non-member countries).

63. *Explanatory Memorandum to Recommendation No. R (92) 1 of the Committee of Ministers to Member States on the Use of Analysis of Deoxyribonucleic Acid (DNA) Within the Framework of the Criminal Justice System*, ¶ 49 (Feb. 10, 1992), available at <https://wcd.coe.int/wcd/ViewDoc.jsp?id=611937&Site=CM>.

64. *Marper*, 2008 Eur. Ct. H.R. ¶¶ 45–47.

65. *Id.* ¶ 37.

66. *Id.* ¶ 36.

2. The *S. & Marper v. the United Kingdom* Decision

On December 4, 2008, the European Court of Human Rights unanimously decided the case of *S. & Marper v. the United Kingdom*.⁶⁷ In that case, the Grand Chamber determined that retaining DNA samples from two individuals who were arrested but not convicted constituted a violation of their privacy rights.⁶⁸ The court in *Marper* raised a number of concerns about broad retention of DNA samples.⁶⁹ It concluded that “the retention of both cellular samples and DNA profiles discloses an interference with the applicants’ right to respect for their private lives, within the meaning of Article 8 § 1 of the Convention [for the Protection of Human Rights and Fundamental Freedoms].”⁷⁰ The court ultimately determined that England’s indefinite retention policy violated Article 8 of the Convention because it interfered with the applicants’ “right to respect for private life” more than was necessary.⁷¹

3. Responses to *Marper*: Changing Approaches to DNA Retention

In response to the *Marper* decision, the United Kingdom Home Office⁷² released a paper, the Home Office Consultation, containing proposed changes and seeking comment from the public.⁷³ The objective was to “develop a DNA framework which has the support and confidence of the public and achieves a proportionate balance between the rights of the individual and protection of the public.”⁷⁴ In the Home Office Consultation, the government analyzed data regarding recidivism, rearrest, and reconviction in both the United States and the United Kingdom to determine the optimal timeframe for retention.⁷⁵ In coming to their final conclusions, the Home Office primarily relied upon a report from the Jill Dando Institute,⁷⁶ which provided data regarding the rates at which arrestees reoffend in

67. *Id.*

68. *Id.* ¶ 125.

69. *Id.* ¶¶ 122–24.

70. *Id.* ¶ 77.

71. *Id.* ¶ 125.

72. The Home Office is the government department responsible for policy and criminal matters in the United Kingdom. *About Us*, HOME OFF., <http://www.homeoffice.gov.uk/about-us> (last visited Mar. 24, 2011).

73. HOME OFFICE CONSULTATION, *supra* note 59, ¶¶ 1.1–1.3.

74. *Id.* ¶ 1.3.

75. *See id.* ¶¶ 6.5–6.13 (discussing findings related to recidivism and reasonable retention periods).

76. The University London College Jill Dando Institute of Crime Science is a department devoted to reducing crime through research and policy analysis. *About the UCL Jill Dando Institute of Crime Science*, UCL JILL DANDO INST. OF CRIME SCI., <http://www.jdi.ucl.ac.uk/about/jdi/index.php> (last visited Mar. 24, 2011).

comparison with the general population and individuals who are convicted.⁷⁷ The report provided an important resource upon which the Home Office based its recommendations for determining the appropriate retention periods for DNA samples.⁷⁸ Ultimately, the Home Office distinguished between retention of DNA samples and retention of DNA profiles.⁷⁹ Due to the greater amount of sensitive and personal information that can be obtained from DNA samples, the Home Office proposed retaining them for no longer than six months.⁸⁰

Although its efforts are admirable, the Home Office still appears to be struggling to obtain full public support for its policies.⁸¹ Some officials, on the other hand, argue that the proposals are adequate, but that they will lead to a reduction in crime solving.⁸² Ultimately, the goal must be to balance the privacy interests of individuals, who should be considered innocent until proven guilty, against the need to solve crimes and prevent future offenses.⁸³ Although England and Wales were at the forefront of DNA collection, the practice has grown increasingly common in the United States, with many of the same issues beginning to emerge.⁸⁴

C. *The United States and Forensic Science Legislation*

1. History of DNA in the United States

Although DNA-based genetic profiling in a criminal investigation was first used successfully by Alec Jeffreys in the United Kingdom in 1987,⁸⁵ debate exists over when DNA evidence was first utilized in

77. See HOME OFFICE CONSULTATION, *supra* note 59, ¶¶ 2.8, 6.5 (presenting research by the Jill Dando Institute regarding the risk of reoffending).

78. See *id.* (noting the report's reliance on the data from the Jill Dando Institute to select retention periods).

79. *Id.* ¶¶ 5.1–5.2.

80. HOME OFFICE, KEEPING THE RIGHT PEOPLE ON THE DNA DATABASE: SCIENCE AND PUBLIC PROTECTION: SUMMARY OF RESPONSES, PUBLIC CONSULTATION 7 (May – 7 August 2009) 12 (2009), <http://www.parliament.uk/deposits/depositedpapers/2009/DEP2009-2788.pdf> [hereinafter Home Office Response].

81. See, e.g., *Time Limits on Innocent DNA Data*, BBC NEWS, May 7, 2009, <http://news.bbc.co.uk/2/hi/uk/8037042.stm> (discussing how rights groups believe the proposals do not adequately address the concerns raised by the *Marper* decision).

82. See *id.* (“One official estimate suggests there will be 4,500 fewer offences detected on average each year . . .”).

83. See *supra* Part III.C (discussing the risks of indefinite retention policies).

84. See, e.g., FLA. STAT. § 943.325 (West 2010) (permitting the collection of DNA samples from arrestees and imposing a burdensome procedure for the removal of such information).

85. See Bieber, *supra* note 13, at 27 (discussing the history of forensic profiling for individual identification). Jeffreys, a professor at the University of Leicester, compared DNA profiles prepared from evidence collected at two different crime scenes

the United States.⁸⁶ There is, however, generally a consensus that DNA evidence became increasingly visible in the United States in the late 1980s in conjunction with three cases.⁸⁷ The first case was a November 6, 1987 conviction in Florida of an individual with evidence from a DNA test.⁸⁸ The second case, tried in New York in 1987, was one of the first in which DNA forensics was legitimized as scientifically valid upon appeal.⁸⁹ The third case occurred in Virginia in response to a series of murders that took place between 1983 and 1987, and the perpetrator became the first individual put to death primarily as a result of DNA evidence.⁹⁰ Since these cases, scientists have made numerous advances in the use of DNA to both exonerate and convict individuals accused of crimes.⁹¹

As police reliance on DNA analysis increased, Congress passed the DNA Analysis Backlog Elimination Act of 2000, authorizing federal law enforcement officials to collect DNA samples from federal offenders convicted of qualifying offenses.⁹² According to Congress, the Act provided legal authority for mandatory and discretionary collection of DNA from federal offenders, and it aimed to improve the effectiveness of DNA processing through a grant program.⁹³ The grant program allocated federal funds in order to deal with a backlog in processing caused by deficiencies in resources at the state and local levels and established the need to carry out DNA testing in a timely manner.⁹⁴ In 2001, additional qualifying offenses were added under §

to the DNA of a false confessor and to DNA collected from adult males living in the area of the crime. *Id.*

86. See, e.g., *id.* (“[P]erhaps the first forensic use of polymerase chain reaction (PCR)-based DNA typing was to assist a Pennsylvania court in a 1986 case [*Commonwealth v. Pestinikas*] in determination of whether two autopsy samples were derived from the same person.”).

87. LINDA L. MCCABE & EDWARD R.B. MCCABE, *DNA: PROMISE AND PERIL* 117–18 (2008).

88. *Id.* In this case, Tommie Lee Andrews was ultimately convicted of rape after the DNA from his blood sample matched the DNA in the semen recovered from the victim. *Id.*

89. *Id.* at 118.

90. *Id.* at 118–19.

91. See, e.g., David Lazer, *Introduction to DNA AND THE CRIMINAL JUSTICE SYSTEM*, *supra* note 13, at i, iv–vii (describing cases in which DNA evidence was used for the purposes of exoneration and conviction).

92. See DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106–546, §§ 1–3, 114 Stat. 2726, 2726–31 (2000) (codified as amended at 42 U.S.C. § 14135) (setting out the purpose of the Act and describing the grant distribution program); see also Regulations Under the DNA Analysis Backlog Elimination Act, 66 Fed. Reg. 34,362 (proposed June 28, 2001) (to be codified at 28 C.F.R. pt. 28) (specifying the qualifying offenses and the responsibilities of the Federal Bureau of Prisons and the FBI under the DNA Analysis Backlog Elimination Act).

93. DNA Analysis Backlog Elimination Act of 2000 §§ 1–3.

94. *Id.*

503 of the USA PATRIOT Act.⁹⁵ DNA collection was further expanded pursuant to § 203(b) of the Justice for All Act of 2004, which allowed for collection of samples from all convicted felons.⁹⁶ Perhaps the largest expansion of DNA collection authority came in 2005. Pursuant to the DNA Fingerprint Act of 2005, federal officers now have the authority to immediately take DNA from any arrestee or detained non-citizen and upload it to the FBI's Combined DNA Index System (CODIS) database.⁹⁷ Once collected, the DNA sample itself is stored in local databases, and DNA profiles are entered into CODIS.⁹⁸

The FBI established CODIS in 1990 as a pilot program and formalized it in 1994.⁹⁹ CODIS contains two sets of searchable information: DNA profiles of convicted individuals (the Convicted Offender Index) and profiles generated from DNA collected at crime scenes (the Forensic Index).¹⁰⁰ In addition to DNA profiles, CODIS also stores information to identify the source of the DNA and the laboratory at which it was analyzed.¹⁰¹ Furthermore, all fifty states have passed laws creating similar, state-run DNA databases.¹⁰² Through CODIS, federal, state, and local crime laboratories can exchange and compare DNA profiles electronically.¹⁰³ This allows law enforcement to identify criminals who commit crimes across state

95. USA PATRIOT Act, Pub. L. No. 107-56, § 503, 115 Stat. 272, 364 (2001); *see also* Regulations Under the DNA Analysis Backlog Elimination Act of 2000, 68 Fed. Reg. 74,855 (Dec. 29, 2003) (to be codified at 28 C.F.R. pt. 28) (providing the Department of Justice's publication of a final rule implementing the qualifying offenses provided under the USA PATRIOT Act). The additional qualifying offenses include the attempt, commission, or conspiracy to commit crimes of violence, as defined in § 16, or federal crimes of terrorism, as defined by § 2332b(g)(5)(B) of Title 18 of the United States Code. Regulations Under the DNA Analysis Backlog Elimination Act of 2000, 68 Fed. Reg. at 74,855-57.

96. Justice for All Act of 2004, Pub. L. No. 108-405, § 203(b), 118 Stat. 2260, 2270 (2004); *see also* DNA Sample Collection from Federal Offenders Under the Justice for All Act of 2004, 70 Fed. Reg. 4763 (proposed Jan. 31, 2005) (to be codified at 28 C.F.R. pt. 28) (providing the Department of Justice's implementation of the Act's authority under an interim final rule).

97. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1004, 119 Stat. 2960, 3085 (2005); *see also* Ryan Singel, *Feds to Collect Millions of DNA Profiles Yearly, Stay Out If You Can*, WIRED (May 12, 2008, 5:15 PM), <http://www.wired.com/threatlevel/2008/05/feds-to-collect> ("Thanks to an amendment in the Violence Against Women Act of 2005 . . . the feds now have the authority to immediately take DNA from any arrestee or 'detained' non-citizen and immediately upload it to the FBI's CODIS database.")

98. See 42 U.S.C. § 14132 (2006) (giving the director of the FBI authority to create a DNA database).

99. Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy*, 34 J.L. MED. & ETHICS 153, 154 (2006).

100. KOBILINSKY ET AL., *supra* note 2, at 164.

101. *Id.*

102. Lazer, *supra* note 91, at xi.

103. KOBILINSKY ET AL., *supra* note 2, at 164-65; Rothstein & Talbott, *supra* note 99, at 154.

lines.¹⁰⁴ Moreover, CODIS is compatible with databases in Europe and South America, making it possible for law enforcement to track and catch criminals even if they commit crimes in different parts of the world.¹⁰⁵

As of 2010, twenty-four states had enacted legislation to require DNA collection from certain felony arrestees, and twelve states and the federal government allowed DNA samples to be collected from all felony arrestees.¹⁰⁶ Of these states, only eight provide for automatic expungement of DNA samples, while seventeen will remove DNA information from the database upon request and, in some cases, at the discretion of law enforcement.¹⁰⁷ At the federal level, DNA is not expunged unless the arrestee submits a request and provides a certified copy of a final court order, signed by a judge, establishing that the charge was dismissed, resulted in an acquittal, or that no charge was filed within the applicable time period.¹⁰⁸

The U.S. military also conducts DNA collection as part of its routine practices and requires all uniformed personnel to provide reference blood samples, either when they enter the military or prior to deployment, from which DNA can be extracted.¹⁰⁹ Although the intended purpose of these samples is to identify human remains,¹¹⁰ Department of Defense regulations have also always allowed the DNA to be used in conjunction with evidence collected at a crime scene.¹¹¹

Another avenue of DNA collection occurs at the local level, and these DNA samples are often not subject to the same oversight as state and federal databases. For example, the district attorney in Orange County, California has begun offering incentives, including the possibility of charges being dropped, to arrestees to obtain DNA

104. KOBILINSKY ET AL., *supra* note 2, at 164–65.

105. *Id.* at 163.

106. *State DNA Database Laws Qualifying Offenses*, DNAResource.com, <http://www.dnaresource.com/documents/statequalifyingoffenses2010.pdf> (last visited Mar. 24, 2011) (charting state DNA database laws as of September 2010); *State Laws for Arrestee DNA Databases*, DNARESOURCE.COM, <http://www.dnaresource.com/documents/ArresteeDNA Laws-2010.pdf> (last visited Mar. 24, 2011); *see also, e.g.*, FLA. STAT. § 943.325 (West 2010) (mandating DNA sample collection from all felony arrestees).

107. *State Laws for Arrestee DNA Databases*, *supra* note 106. In Minnesota, DNA samples are automatically expunged upon a finding of not guilty, or at the request of the individual if the charges were dismissed or dropped. *Id.*

108. *CODIS—Expungement Policy*, FBI—FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/codis/codis_expungement (last visited Mar. 24, 2011); *State Laws for Arrestee DNA Databases*, *supra* note 106.

109. Bieber, *supra* note 13, at 43.

110. *Id.*

111. *See id.* at 44 (noting that Department of Defense regulations allow access to blood samples for DNA profiling during criminal investigations).

samples and expand the county's DNA database.¹¹² Critics are concerned that the district attorney's plan targets individuals arrested for nonviolent misdemeanors,¹¹³ a category of arrestees that previously had not been required to provide DNA samples under any state or federal legislation. The DNA samples collected in Orange County are maintained in a local database and are not run by an accredited crime lab.¹¹⁴ Critics call these types of local databases "rogues" because they are not subject to state and federal guidelines and thus lack the same safeguards against misuse of the DNA profiles.¹¹⁵

There are now a variety of circumstances under which an individual suspected of a crime may be asked or forced to provide a DNA sample. That sample may then find its way onto DNA databases at the federal and local levels. The increasing number of cases relying on DNA evidence has thus forced courts to address circumstances in which it is appropriate not only to collect DNA samples from a suspect but to introduce the resulting profiles as evidence.

2. Judicial Decision-Making Regarding DNA

Courts have held that, even where a DNA profile has not been matched to a specific individual, it can be used to identify a suspect on an arrest warrant for purposes of fulfilling the "reasonable certainty" identification requirements. However, once DNA has been collected, processed, and used to identify a suspect, many factors can affect how and when prosecutors can introduce the information into evidence against a criminal defendant. Courts have established standards for when scientific evidence is admissible and can be presented to a jury. In *Frye v. United States*,¹¹⁶ the District of Columbia Court of Appeals was the first to elucidate a standard for the admission of scientific evidence.¹¹⁷ Under the *Frye* standard, evidence must be "generally accepted" in the pertinent scientific community to be admissible in court.¹¹⁸ Although some states

112. See Tami Abdollah, *Arrested in O.C.? A DNA Sample Could Buy Freedom*, L.A. TIMES, Sept. 17, 2009, at A1 (noting that, in some cases, charges may not even be filed if the arrested person agrees to provide a DNA sample).

113. *Id.*

114. *Id.*

115. *Id.*

116. *Frye v. United States*, 293 F. 1013, 1014 (D.C. Cir. 1923).

117. *Id.*; see also KOBILINSKI ET AL., *supra* note 2, at 198–200 (describing *Frye* and "the creation of a judicial gatekeeping function").

118. *Frye*, 293 F. at 1013.

continue to adhere to the *Frye* standard,¹¹⁹ the introduction of the Federal Rules of Evidence¹²⁰ and the Supreme Court's decision in *Daubert v. Merrell Dow Pharmaceuticals*¹²¹ further expanded the discretion of judges to determine the admissibility of scientific evidence. Under *Daubert*, courts must determine the admissibility of scientific evidence by evaluating the validity of two aspects: whether the evidence represents "scientific knowledge" and whether it is relevant and supports what the evidence purports to show.¹²² In determining whether evidence represents scientific knowledge, a court may consider whether it is testable, if it has been described in scientific publications subject to peer review, its reliability, and its general acceptance in the relevant community.¹²³ Although originally limited to scientific evidence, in 1999, the Supreme Court extended *Daubert* to apply to all expert testimony in which technical or specialized material is presented.¹²⁴ In practice, DNA evidence is usually found admissible under these standards, but issues may arise because of improper chain of custody practices or contamination.¹²⁵

In addition to admissibility concerns, courts have also had to grapple with whether DNA collection and retention is permissible under the Constitution. Analysis of DNA collection laws in the United States has focused on their constitutionality under the Fourth Amendment.¹²⁶ The Ninth and Tenth Circuits have addressed the question of whether the DNA Act is a valid exercise of congressional power, and each determined that it is constitutionally permissible.¹²⁷

119. See KOBILINSKY ET AL., *supra* note 2, at 206 ("The standards adopted by the individual states tend to be derivatives of one of the three federal standards The majority use the *Frye* standard.").

120. See FED. R. EVID. 403 ("Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."); see also KOBILINSKY ET AL., *supra* note 2, at 201 (describing how Rule 403 expanded the gatekeeping function of judges).

121. *Daubert v. Merrell Dow Pharm.*, 509 U.S. 579, 592–96 (1993) (allowing judges to look beyond general acceptance and consider other factors in deciding whether or not to admit expert testimony).

122. *Id.* at 592–94.

123. *Id.* at 592–96.

124. See *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 158 (1999) (concluding that the general holding of *Daubert* applies to technical and other specialized knowledge such as the testimony of engineers, as well as to scientific knowledge).

125. KOBILINSKY ET AL., *supra* note 2, at 207–08.

126. See, e.g., *United States v. Kincade*, 379 F.3d 813, 821 (9th Cir. 2004) (finding that DNA collection cases implicate the Fourth Amendment because the "compulsory extraction of blood . . . constitutes a 'search' within the meaning of the Constitution").

127. See *id.* at 839–40 (discussing the case of a convicted felon who refused to have his blood drawn as a condition of probation and upholding searches pursuant to the DNA Act as constitutional); *United States v. Plotts*, 347 F.3d 873, 877 (10th Cir. 2003) (finding that the DNA Act was a "legitimate exercise of congressional power

Additionally, a number of states have ruled on Fourth Amendment challenges to local statutes, and the majority have treated DNA collection as something akin to fingerprinting, a practice that courts have long accepted.¹²⁸ Conversely, a Minnesota appellate court ruled that a statute requiring officers to obtain a sample of DNA from arrestees was unconstitutional because a person who is merely charged with a crime has a greater expectation of privacy than someone who was convicted.¹²⁹ This demonstrates that some courts will indeed be willing to rule against DNA collection practices, particularly when it seems improbable that taking the DNA sample will produce evidence of a crime.¹³⁰

D. *Alternative DNA Collection Practices*

Although the largest DNA databases are run by the United Kingdom and the United States, a number of other countries utilize DNA forensics as a crime-solving tool. Many of these countries have implemented more restrictive DNA collection practices that can serve as a model for the United States and the United Kingdom. Furthermore, countries are becoming increasingly capable of sharing DNA profile information, so it is important to understand what information might be available from these various databases.

In New Zealand, the use of DNA profiling in two high-profile sex offender cases in the early 1990s prompted the creation of a DNA database.¹³¹ In 1995, the New Zealand police began collaborating with the Institute of Environmental Science and Research, Ltd., and the legislature established the New Zealand DNA Databank in August 1996.¹³² The Criminal Investigations (Blood Samples) Act of 1995 establishes stringent standards under which police can collect

under the Necessary and Proper Clause"); *see also* United States v. Reynard, 473 F.3d 1008, 1021–22 (9th Cir. 2007) (holding that the DNA Act did not go beyond Congress's power under the Commerce Clause or the Fifth Amendment right against self-incrimination).

128. *See, e.g.*, United States v. Pool, 645 F. Supp. 2d 903, 906 (E.D. Cal. 2009) (upholding the constitutionality of DNA sample collection from individuals arrested for felonies in California, when the DNA is to be used solely for "criminal law enforcement, identification purposes"); Anderson v. Commonwealth, 650 S.E.2d 702, 705 (Va. 2007) (holding that the taking of an individual's DNA upon arrest is "no different in character than acquiring fingerprints upon arrest" and does not constitute an unlawful search under the Fourth Amendment).

129. *In re* C.T.L., 722 N.W.2d 484, 492 (Minn. Ct. App. 2006).

130. *See id.* (holding that an individual who has not been convicted maintains a reasonable expectation of privacy, and thus the Fourth Amendment is violated when a biological specimen is taken from such a person, unless "there is a fair probability that the search will produce contraband or evidence of a crime").

131. SA Harbison et al., *The New Zealand DNA Databank: Its Development and Significance as a Crime Solving Tool*, 41 SCI. & JUST. 33, 34 (2001).

132. *Id.* at 33–34.

blood samples for inclusion in the databank.¹³³ Under the Act, suspects may voluntarily provide a sample or, in certain situations, the High Court may compel them to do so for comparison to a particular case.¹³⁴ Additionally, all individuals who are convicted of an indictable offense must provide a sample for the databank.¹³⁵ The Act also specifically mandates that individuals who voluntarily provide a sample for inclusion on the databank may choose to have the DNA profile removed at any time.¹³⁶ When drafting the Act, New Zealand took into consideration individual rights, the rights of police to obtain samples, and the potential for misuse of data.¹³⁷ As a result, some might consider its potential more limited in scope than the United Kingdom's program. Despite this limitation, New Zealand has had a great deal of success with the databank, which contains over 13,000 individual profiles.¹³⁸ The databank has been particularly helpful with identifying suspects in unsolved burglary cases,¹³⁹ and it continues to develop as law enforcement and legislators gain experience while maintaining the databank's original objectives and aims.¹⁴⁰

In Canada, a National DNA Data Bank was officially established in 2000.¹⁴¹ In 2005, Canada further expanded the data bank to allow for the inclusion of DNA profiles from "all persons convicted before June 30, 2000 of murder, manslaughter or a sexual offence."¹⁴² Like New Zealand, Canada's data bank does not include profiles from arrestees.¹⁴³ Additionally, in most cases, courts must authorize the collection of DNA from convicted individuals.¹⁴⁴ However, a court may decline to authorize the collection if it determines that "a DNA order would adversely affect the individual's privacy and security interests in a manner that is grossly disproportionate to the public interest."¹⁴⁵ For example, in *R. v. R.C.*, a juvenile stabbed his mother in the foot with a pen after she dumped dirty laundry on him; the

133. *Id.* at 34.

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.* at 35.

139. *See id.* at 36 ("Of the total number of reported 'hits' 77% have originated from burglaries.").

140. *Id.* at 37.

141. *DNA Data Bank*, PUB. SAFETY CAN., <http://www.publicsafety.gc.ca/prg/cor/tls/dna-eng.aspx> (last visited Mar. 24, 2011).

142. *Id.*

143. *Id.*

144. *See R. v. R.C.*, [2005] 3 S.C.R. 99, para. 19 (Can.) (noting that § 487.051(1)(a) of the Criminal Code requires a court to authorize the taking of DNA samples from a person convicted of a primary designated offense unless certain conditions are met).

145. *Id.* para. 21.

juvenile pled guilty to assault with a weapon.¹⁴⁶ In considering whether it was appropriate to authorize the taking of a DNA sample, the trial judge balanced the objectives of DNA retention against the principles and objectives of the youth criminal justice legislation.¹⁴⁷ The trial judge ultimately refused to issue an order to authorize the DNA collection, and the appellate court affirmed his decision.¹⁴⁸ This policy demonstrates a scheme in which it is feasible and appropriate to give increased discretion to trial courts regarding DNA collection and retention decisions.

On a broader scale, Interpol has recognized the increasing usefulness of DNA databases and established a system known as the DNA Gateway, through which police in member countries can submit DNA profiles from offenders, crime scenes, missing persons, and unidentified bodies to Interpol's automated DNA database.¹⁴⁹ At the same time, the protocol states that member countries retain ownership over the DNA profiles and over other countries' access to the data.¹⁵⁰ The national laws of individual countries continue to govern the destruction of DNA profiles submitted to the Gateway.¹⁵¹ The DNA Gateway has been very successful; in its first six years of operation, more than 100,000 DNA profiles were contributed by fifty-five member countries and in 2009, searches of the database by member countries led to seventy-four international hits.¹⁵² This adds another level of consideration regarding DNA collection policies, as arrestees whose DNA is retained in a database can now potentially be implicated in cases at an international level.

III. ANALYSIS

DNA is admittedly a powerful tool in solving crimes that might otherwise remain unsolved.¹⁵³ In September 2005, Sally Anne Bowman's body was discovered in South London following her brutal sexual assault and murder.¹⁵⁴ Although the killer was not

146. *Id.* para. 1.

147. *See id.* para. 33 (explaining that the court must strike a balance between youth criminal justice legislation and other DNA order provisions of the law).

148. *Id.* paras. 11–14.

149. INTERPOL, COM/FS/2010-09/FS-01, DNA PROFILING 1, <http://www.interpol.int/Public/ICPO/FactSheets/FS01.pdf>.

150. *Id.*

151. *Id.*

152. *Id.*

153. *See, e.g.*, Philippe Naughton, *Britain Needs DNA Database, Says Officer Who Headed Sally Anne Murder Inquiry*, TIMES (London), Feb. 22, 2008, <http://www.timesonline.co.uk/tol/news/uk/crime/article3416427.ece> (describing the case of a woman whose killer was brought to justice by chance after his DNA was taken nine months after the murder, following an arrest for a minor bar fight).

154. *Id.*

immediately apprehended, he was identified nine months later after his DNA was taken following a "minor scuffle."¹⁵⁵ Even the Sally Anne Bowman case, however, lends only questionable support for retaining the DNA of individuals who are arrested but not convicted of crimes. The killer in that case had a number of prior convictions,¹⁵⁶ so even more restrictive legislation would likely have allowed for his DNA to be retained on a database.

As discussed above, existing and potential legislation surrounding DNA collection and retention can essentially be broken down into the following four categories: (1) collection of DNA only from individuals who are charged and convicted of crimes; (2) DNA collection from arrestees with indefinite retention of DNA profiles on a database; (3) DNA collection from arrestees with removal of DNA profiles upon request; and (4) DNA collection from arrestees with automatic expungement.

A. Privacy Concerns

The idea of privacy can encompass a number of different interests, including the right to have control over personal information about oneself, freedom from surveillance, freedom to make personal decisions absent the influence of others, and the right to exclude others from one's personal things and places.¹⁵⁷ The benefits and dangers of DNA collection stem from the amount of information it can reveal about individuals, including their propensity for certain diseases and to whom they are related.¹⁵⁸ Thus, experts raise concerns about who should control genetic information, given that it can be used to reveal information about relatives in addition to the individual from whom a sample was taken.¹⁵⁹ DNA molecules are like a medical record, but DNA sequence profiles contain information that raises additional privacy concerns.¹⁶⁰ One U.S. court that addressed whether constitutional rights to privacy were implicated by genetic testing held that "the right to privacy protects against the collection of information by illicit

155. *Id.*

156. *Id.*

157. See George J. Annas, *Genetic Privacy, in* DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 13, at 135, 136 (defining the concept of privacy).

158. *Id.* at 137 ("DNA has the paradoxical quality of being unique to an individual, yet shared with others."); Lazer, *supra* note 91, at 9 ("[DNA] may reveal where you have been. It may reveal what you look like. It may reveal your propensity for getting a particular disease. It reveals who you are related to and may reveal your relatives' propensity for getting a particular disease.").

159. LAURIE, *supra* note 44, at 93.

160. Annas, *supra* note 157, at 136.

means as well as unauthorized disclosures to third parties”¹⁶¹ Given that DNA profiling is utilized around the world to study diseases and for diagnostic testing in hospitals,¹⁶² the system needs adequate safeguards to protect against the use of DNA information for unauthorized purposes.

The National DNA Database in the United Kingdom was used for research without the consent of the individuals involved.¹⁶³ It is unacceptable to carry out medical research on individuals without their consent, and even criminals do not relinquish their right to consent to having medical research conducted on them merely because they were convicted of a crime.¹⁶⁴ Another case that raised particular controversy in the United Kingdom was the retention of a DNA sample collected from an infant on a national police database.¹⁶⁵ The DNA sample was taken to eliminate the baby’s DNA as a possible match from crime scene evidence, but was not immediately removed after this use and was thus accessible during later law enforcement searches.¹⁶⁶ Similarly, in the United States, the director of the Texas Civil Rights Project discovered that newborn blood samples taken for medical purposes were sent to the military for potential use in a database for law enforcement purposes.¹⁶⁷ This action raises concerns about law enforcement capitalizing on DNA collected from individuals who have clearly committed no crimes to expand a *criminal* DNA database. As one critic has noted, “If the government wants a universal DNA database it should say so, not smuggle one in through the backdoor.”¹⁶⁸

Law enforcement can similarly capitalize on this backdoor strategy through the ability of DNA to provide information about not just an individual, but also about his or her family members. Although using DNA to identify kin has primarily been used in mass

161. *Id.* at 138 (citing *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998)).

162. See, e.g., Bieber, *supra* note 13, at 42 (discussing the DNA Sciences Gene Trust Project, which registers thousands of participants in the United States to identify the links between genes and common diseases).

163. Mairi Levitt, *The National DNA Database: Why No Public Debate?*, in 3 ETHICS, LAW, AND SOCIETY 215, 216 (Jennifer Gunning & Soren Holm eds., 2007) (noting that the database also contained DNA profiles from children and innocent individuals).

164. *Id.*

165. *Baby’s DNA Was Held on Database*, BBC NEWS, Mar. 9, 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/7933753.stm.

166. *Id.*

167. Mary Ann Roser, *Suit Possible Over Baby DNA Sent to Military Lab for National Database*, STATESMAN (Austin, Tex.), Feb. 22, 2010, <http://www.statesman.com/news/texas-politics/suit-possible-over-baby-dna-sent-to-military-268714.html>.

168. *Liberty Government Defeat on DNA Database*, BBC NEWS, Nov. 5, 2008, http://news.bbc.co.uk/2/low/uk_news/politics/7710310.stm (quoting Shami Chakrabarti).

disaster and missing person identifications,¹⁶⁹ DNA was also used in cases in the United Kingdom¹⁷⁰ and the United States¹⁷¹ to identify relatives of potential suspects. State and federal statutes in the United States do not specifically address the use of DNA databases to identify family members, so the inclusion of the DNA of arrestees may also lead to the “de facto inclusion” of kin through familial searching procedures.¹⁷² One expert has cautioned that “DNA patterns from close relatives . . . have a greater chance of matching than do those from randomly selected, unrelated individuals, and this is often important to consider in statistical analyses of DNA testing results.”¹⁷³ Another risk of these types of searches lies in the fact that, although identical twins have different fingerprints, they have identical genomes.¹⁷⁴ Thus, an individual with an identical twin may be erroneously implicated in a crime merely because the individual’s sibling had previously been arrested.¹⁷⁵ Notably, tests carried out on behalf of the California police authorities showed that the misidentification of two people having the same DNA profile was as high as one in ten thousand.¹⁷⁶ Such findings demonstrate that despite the advancements that have been made, DNA technology is not infallible.

B. *Innocent Until Proven Guilty*

The criminal justice systems of both the United Kingdom and the United States are based upon the presumption that individuals are innocent until proven guilty.¹⁷⁷ As a result, the *Marper* court was particularly concerned with the fact that it “was an entirely improper and prejudicial differentiation to retain materials of persons who

169. Frederick R. Bieber et al., *Finding Criminals Through DNA of Their Relatives*, SCIENCE, June 2, 2006, at 1315, 1315.

170. *See id.* (describing a Wales case where “[a] search of the U.K. National DNA Database for individuals with a single specific rare allele found in the crime scene evidence . . . identified a 14-year old boy with a similar overall DNA profile[, which] led police to his paternal uncle, Jeffrey Gafoor”).

171. *See id.* (describing a 1984 murder case where the police located their suspect by matching DNA found on the scene to DNA of his brother, found on the North Carolina DNA offender database).

172. *See id.* at 1316 (noting that the ability to conduct familial searches creates “a new category of people [who] effectively would be placed under lifetime genetic surveillance”).

173. Bieber, *supra* note 13, at 41.

174. KOBILINSKY ET AL., *supra* note 2, at 6.

175. *See* Bieber, *supra* note 13, at 41 (“[R]outine analysis of nuclear DNA polymorphisms cannot distinguish between monozygotic twins (triplets, quadruplets, and so on). Thus, a so-called DNA match, although inclusionary, is not necessarily probative.”).

176. DAVIES ET AL., *supra* note 16, at 97.

177. *See infra* Part III.B (discussing presumption of innocence policies in various countries).

should be presumed to be innocent.”¹⁷⁸ In the United Kingdom, the majority of respondents to the Home Office’s Consultation report were against retaining samples of individuals who were arrested but not charged or convicted.¹⁷⁹ Additionally, the *Marper* court noted that there is a “risk of stigmatization, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offense and are entitled to the presumption of innocence, are treated in the same way as convicted persons.”¹⁸⁰ Every person has a right not only to be presumed innocent, but also to be absolved of any suspicion regarding his or her innocence following acquittal.¹⁸¹

This presumption of innocence is so important that it has been codified by a number of countries.¹⁸² A prominent example can be found in the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe, which states, “Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.”¹⁸³ Local U.S. governments should take this into consideration when drafting their own DNA retention policies, particularly given the value that U.S. citizens place on their privacy and on the right to a presumption of innocence.¹⁸⁴ Enacting more permissive legislation regarding the retention of DNA from arrestees who are not convicted undermines this right.

Furthermore, allowing retention of arrestees’ DNA may influence law enforcement to target individuals who they believe may commit crimes in the future, but who are currently innocent. In the United Kingdom, for example, at least one officer admitted that he was targeting certain juveniles who had not yet been arrested as part of a

178. *S. & Marper v. United Kingdom*, 2008 Eur. Ct. H.R. 1581, ¶ 127.

179. HOME OFFICE RESPONSE, *supra* note 80, ¶ 2.1.

180. *Marper*, 2008 Eur. Ct. H.R. ¶ 122.

181. *See id.* (“[The applicants’] perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offense are required to be destroyed.”).

182. *See, e.g.*, Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c. 11(d) (U.K.) (“Any person charged with an offence has the right to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal.”); 1789 Declaration des droits de l’Homme et du citoyen [Declaration of the Rights of Man and of the Citizen] art. 11. (“Everyone is supposed innocent until having been declared guilty.”).

183. Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe, art. 6.2, Nov. 4, 1950, 213 U.N.T.S. 221.

184. *See* U.S. CONST. amends. IV–VI, XIV (establishing a right to be free from unreasonable government searches and seizures, a right to due process of law, and a right to a speedy trial by jury in criminal cases, and making these rights applicable against state and local governments); *see also* Coffin v. United States, 156 U.S. 432, 453 (1895) (establishing the presumption of innocence for individuals accused of crimes).

“long-term crime prevention strategy.”¹⁸⁵ If police begin using DNA databases in this way, then they are effectively making determinations of guilt against individuals who have done nothing wrong.¹⁸⁶ These practices become even more potentially hazardous when considered in the context of DNA systems that retain profiles from arrestees indefinitely or for extended periods of time.

C. *The Implications of Indefinite Retention of DNA Profiles*

Indefinite retention policies are the most vulnerable to attack because they raise the greatest amount of concern, particularly when DNA is collected from individuals who have not been convicted of any crime. Most countries are opposed to indefinite retention, choosing to remove DNA profiles after five to twenty years if an individual is convicted, or immediately if the individual is acquitted or the charges are dropped.¹⁸⁷ Before the *Marper* decision, only England and Wales, Austria, Finland, and Norway retained the DNA profiles of convicted individuals indefinitely.¹⁸⁸ Even England and Wales are now being forced to cabin their policies by weighing the public benefit against private intrusions.¹⁸⁹

A removal upon request policy increases the likelihood that individuals will be informed that they have the option to have their DNA profiles removed from a database. One benefit of such a policy is that it gives arrestees a forum for objecting to the retention of their DNA. However, some critics have raised concerns over the reluctance of law enforcement and other responsible authorities to respond to removal requests. Figures obtained under the Freedom of Information Act showed that some police forces in England and Wales granted 80 percent or more of removal requests, while other forces did not remove the DNA profiles of any applicants, with an average removal rate of 22 percent.¹⁹⁰ One individual who was arrested following a misunderstanding with her husband and against whom charges were never filed has been trying to have her DNA records

185. *Police Target 'Innocent' Youths for Arrest in Bid to Increase DNA Samples on Database*, MAIL ONLINE, June 4, 2009, [http://www.dailymail.co.uk/news/article-1190785/Police-target-innocent-youths-arrest-bid-increase-DNA-samples-data base.html](http://www.dailymail.co.uk/news/article-1190785/Police-target-innocent-youths-arrest-bid-increase-DNA-samples-data-base.html).

186. *See id.* (quoting a representative who commented that “[b]uilding a catalogue of people they think will be prominent criminals in the future sounds like a renegade justice system”).

187. GENEWATCH UK, *THE POLICE NATIONAL DNA DATABASE: BALANCING CRIME DETECTION, HUMAN RIGHTS AND PRIVACY* 28 (2005), <http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/NationalDNADatabase.pdf>.

188. *Id.*

189. *See generally* S. & Marper v. United Kingdom, 2008 Eur. Ct. H.R. 1581.

190. Andy Tighe, *Innocent People Face DNA Database 'Shambles,'* BBC NEWS, Dec. 31, 2009, <http://news.bbc.co.uk/2/hi/8434713.stm>.

removed from the database for over five years.¹⁹¹ Practices such as this not only threaten the privacy interests of innocent individuals, they also undermine public confidence in the police forces.¹⁹² Thus, review policy is important to monitor removal requests and ensure that requests are handled expediently and appropriately within the guidelines.

Although judicial decisions in the United States have primarily analyzed the constitutionality of collecting DNA,¹⁹³ retention policies should also be subject to critical analysis. A Florida statute, for example, provides that individuals from whom DNA is collected upon arrest can only have the sample and information destroyed if they provide official documentation demonstrating that the charges were dismissed or the conviction overturned.¹⁹⁴ However, the burden should instead be placed on the DNA collector to automatically destroy samples from those individuals who are arrested and either not charged or found not guilty.

Additionally, many state statutes appear to authorize indefinite retention of DNA samples from convicted individuals.¹⁹⁵ Particularly in light of the *Marper* decision, states should provide more detailed guidelines and limit the scope of the samples that are maintained in a DNA database. Analysts and legislatures can use available statistics to determine the types of crimes (e.g., sexual assaults) that are typically committed by repeat offenders, and only in those situations is it appropriate to permanently maintain DNA samples in the database. Procedures should also be in place to allow convicted felons to petition to have their DNA removed from the database after a certain period of time.

While most statutes in the United States allow for overly broad collection and retention of DNA samples, some states have implemented more restrictive legislation in their collection practices. The Virginia statute at issue in *Anderson v. Commonwealth* is narrower than those in other states and only imposes the DNA sampling requirement for certain crimes.¹⁹⁶ Additionally, a Minnesota court in *In re C.T.L.* held that a statute requiring officers to obtain a sample of DNA from arrestees was unconstitutional

191. *Id.*

192. *Id.*

193. *See supra* Part II.C.2 (summarizing judicial decisions in the United States regarding DNA collection practices).

194. FLA. STAT. § 943.325(16) (West 2010).

195. *See, e.g., id.* (establishing guidelines for DNA retention in Florida).

196. *See Anderson v. Commonwealth*, 650 S.E.2d 702, 705 (Va. 2007) (providing the text of the statute at issue that enumerates the crimes that would result in collection of DNA from an arrested person).

because it violated the Fourth Amendment.¹⁹⁷ *In re C.T.L.* demonstrates that limiting certain aspects of the federal DNA statute is appropriate, particularly in the case of individuals who are arrested but not convicted.¹⁹⁸ Unlike more expansive views toward DNA retention, these cases provide examples of courts that have taken a more cautious approach to the use of DNA collection to identify and apprehend suspects. By doing this, courts and legislators seem to acknowledge the need to balance the interest in solving crimes with the interest in respecting individuals' privacy.

Despite these outliers, a trend exists toward broadening the use of DNA databases at the local level. In Florida, for example, the legislature recently passed a measure that will require arrested individuals to provide DNA samples for inclusion in a statewide database, even if they are never charged with an offense.¹⁹⁹ This requirement will apply to *all* felony suspects within ten years.²⁰⁰ This bill suggests that legislatures are becoming increasingly concerned with crime control and less concerned with the privacy implications of this type of legislation.

The final response published by the United Kingdom after the *Marper* decision demonstrates its commitment to balancing the need for a DNA database with the protection of individual rights.²⁰¹ Under this new system, law enforcement will remove the profiles of adults arrested, but not charged or convicted of any recordable offense, after six years.²⁰² While a step in the right direction, this proposed solution does not necessarily satisfy immediate privacy concerns. Some statistics indicate that recidivism among individuals convicted of crimes generally occurs within fifteen years,²⁰³ and alternate studies have suggested that the risk of reoffending decreases significantly after as little as two years.²⁰⁴ Thus, it seems unnecessary to retain profiles of individuals who have committed no offense beyond the timeframe in which even those convicted of a crime are considered at significantly less risk of reoffending. Experts further noted that "[l]ong retention of DNA personal data has little to

197. *In re C.T.L.*, 722 N.W.2d 484, 486 (Minn. Ct. App. 2006) (holding that a statute requiring officers to obtain a sample of DNA from arrestees was unconstitutional).

198. *Id.* at 490.

199. FLA. STAT. § 943.325(3) (West 2010).

200. *Id.*

201. See generally HOME OFFICE RESPONSE, *supra* note 80 (addressing concerns regarding the privacy rights of individuals and the need for effective police enforcement).

202. *Id.*

203. *Id.*

204. See *DNA Retention "Justifications" Disproved by Statistics*, TECH & L. BLOG (Nov. 27, 2009), <http://blog.tech-and-law.com/2009/11/dna-retention-disproved-by-statistics.html> (discussing studies conducted by English privacy experts regarding rates of reoffending).

do with detecting ordinary crime.”²⁰⁵ Additionally, a reduction in the length of retention does not eliminate the incentive for police to arrest individuals merely to obtain their DNA given the logic that getting a profile in the system for six years is better than not getting it at all.

Although some advocates believe that maintaining DNA in a universal database will have a deterrent effect on the commission of future crimes,²⁰⁶ at least one official in the United Kingdom has expressed concern that the increased amount of personal, identifying information being collected and retained also leads to a potential increase in the risks of false matches and the potential for technical or human error.²⁰⁷ Consequently, “[t]here is a real risk that a disproportionate number of *innocent* British citizens will be sucked into foreign criminal investigations”²⁰⁸ because they will be incorrectly implicated in conjunction with a crime. Those in favor of expanding DNA databases, however, argue that the benefits that can be gained from using the information to both solve and prevent crimes far outweigh the potential risks. For example, the City of Chicago completed a study in 2005 that looked at the criminal activities of eight individuals who committed a number of violent crimes before finally being arrested.²⁰⁹ The study reportedly found that police could potentially have prevented twenty-two murders, thirty rapes, and an unspecified number of attempted rapes and aggravated kidnappings if they had had access to the DNA profiles of the eight offenders.²¹⁰

Continued expansion of both national and international databases also raises concerns about creating a backlog in the processing of data. Although the situation in the United States has improved, a number of states have reported a backlog in samples collected from crime scenes and offenders,²¹¹ and there is a lack of resources to support the mandate to create DNA databases.²¹² Some have gone so far as to say that every U.K. citizen and visitor should be added to the national DNA database.²¹³ However, given the

205. *Id.*

206. *See, e.g.,* DAVIES ET AL., *supra* note 16, at 97 (discussing how Britain’s implementation of a DNA database “will not only assist crime investigation, but might also be a deterrent in that a person listed might abstain from committing further sexual crimes as the chances of being identified are increased”).

207. *ECHR Decided Against the UK DNA Database*, EUROPEAN DIGITAL RTS. (Dec. 17, 2008), <http://www.edri.org/edri-gram/number6.24/echr-marper-case-dna-uk>.

208. *Id.* (emphasis added).

209. CITY OF CHI., CHICAGO’S STUDY ON PREVENTABLE CRIMES 1–2 (2005), <http://www.dnaresource.com/documents/ChicagoPreventableCrimes-Final.pdf>.

210. *Id.*

211. Cordner & Scarborough, *supra* note 21, at 107.

212. *See* Lazer, *supra* note 91, at xi (“[R]esources have been slow to follow the mandate to create [DNA] databases.”).

213. *All UK ‘Must Be on DNA Database,’* BBC NEWS, Sept. 5, 2007, <http://news.bbc.co.uk/2/hi/uk/6979138.stm>.

difficulties faced by labs in processing and storing DNA profiles, it would be difficult for a country like the United States to attain such a lofty goal successfully. Priority should be placed on ensuring that the DNA of individuals actually convicted of crimes gets entered into the necessary databases before time can be allocated to those arrested but not convicted.

Expanding the population of individuals being included in a database also increases the potential for simple human error to lead to grave mistakes.²¹⁴ Although it reported that many of the mistakes have been corrected, a study released by the U.K. Home Office in August 2007 found approximately 550,000 files with wrongly recorded or misspelled names.²¹⁵ Even more concerning is evidence that the Home Office used falsified information to justify their DNA retention policies on at least one occasion.²¹⁶ David Hanson, the Home Office Minister, attributed the actions to an administrative error,²¹⁷ but even if this is the case, it is unacceptable that DNA databases used to support convictions can be manipulated in such a way as to provide inaccurate information.

IV. SOLUTION

While appearing to be the primary method for governing DNA collection and retention, broad-sweeping legislation is an inappropriate means of mandating DNA collection. Instead, states and the federal government should establish more targeted and specific standards that take into consideration, for example, the policy goals of rehabilitating juvenile offenders, as opposed to merely punishing them. In order to address the concerns raised by the European Court of Human Rights in *Marper* and forestall similar litigation in the United States, legislatures should look to the policies of Scotland and Canada, which have placed an increased emphasis on privacy interests. Under an automatic expungement policy, statutes establish a time period after which officials must remove the DNA profiles of arrestees. Furthermore, some categories of crimes should

214. Cf. *UK DNA Database Errors Raise Concerns*, EUROPEAN DIGITAL RTS. (Dec. 5, 2007), <http://www.edri.org/edrigram/number5.23/uk-dna-database-error> (quoting one investigator who cautioned “[g]overnment databases are not necessarily 100 per cent accurate It is quite clear you can’t trust the Government with your personal information. They need to massively tighten up the way they deal with these issues”).

215. *Id.*

216. Tom Whitehead, *Blunder on DNA Defence by Home Office*, TELEGRAPH (London), Feb. 11, 2010, <http://www.telegraph.co.uk/news/uknews/law-and-order/7215984/Blunder-on-DNA-defence-by-Home-Office.html>.

217. *Id.*

result in DNA removal immediately upon a finding of not guilty or a determination that charges will be dropped.

Research conducted by the Jill Dando Institute following the *Marper* case showed that 52 percent of reoffending happens within six years.²¹⁸ The research also showed that “it takes 15 years before the risk of offending is at the same level as that for the general population.”²¹⁹ However, it is inappropriate to characterize an arrest as an “offense” given the presumption of innocence granted to defendants in the United States and the United Kingdom. Although probable cause is needed for an arrest, that individual still remains innocent until proven guilty. One criticism by the *Marper* court was that “[i]n most of the specific examples provided by the Government the successful prosecution had not been contingent on the retention of the records and in certain others the successful outcome could have been achieved through more limited retention in time and scope.”²²⁰ As a result of these findings, it would be wholly inappropriate to have policies that allow for indefinite retention of DNA profiles. Even under the most generous perspective, the laws should be amended to provide for automatic expungement by the fifteen-year mark, since “[t]wo-thirds of re-offending happens within 12 years.”²²¹ Furthermore, there should be automatic expungement immediately for misdemeanor arrests.

Access to DNA databases should be limited to prevent law enforcement from utilizing familial search procedures to match DNA profiles to crime scene evidence, unless an individual has consented to such a search. While an individual who is arrested for a crime arguably gives up certain rights that could justify collecting and retaining DNA, there is no rationale for extending that to the family members of arrestees. Similarly, individuals who voluntarily provide DNA profiles for medical testing and babies who are automatically screened at birth do not consent per se to inclusion in a criminal database. Thus, any legislation enacted that establishes a database containing DNA profiles from arrestees must contain safeguards to protect DNA profiles from being used for purposes outside of the scope of the consent given by such individuals.

Given the large number of member countries who may also have access to Interpol’s DNA Gateway,²²² U.S. policy should be drafted to reflect an awareness of the fact that placing an individual’s information on a DNA database could subject them to international investigation. Thus, given that arrestees are still considered innocent under U.S. law, this information should not be among that shared

218. HOME OFFICE CONSULTATION, *supra* note 59, ¶ 2.7.

219. *Id.*

220. *S. & Marper v. United Kingdom*, 2008 Eur. Ct. H.R. 1581, ¶ 88.

221. HOME OFFICE CONSULTATION, *supra* note 59, ¶ 2.7.

222. See *supra* notes 149–52 and accompanying text (discussing Interpol’s DNA Gateway which facilitates the sharing of DNA information between member countries).

with other countries. Taking into consideration the European Court of Human Rights's suggestions in *Marper*, courts or legislatures may need to step in and place certain limitations on the trend in the United States toward decreased privacy and increased retention of DNA samples from an expanded population of individuals. Given the expanded role of forensic DNA analysis in criminal cases both in the United States and abroad, the next step seems to be the expansion of global DNA databases. Law enforcement and experts have already recognized the benefit of sharing information from DNA databases to facilitate crime solving. Sharing information internationally increases the possibility for abuse, given the involvement of actors at many different levels and in many different locations. It becomes the responsibility of individual countries to ensure that they do not grant others access to the sensitive personal data of innocent citizens who did not consent to have their data used in this manner.

V. CONCLUSION

The expanded use of DNA databases in criminal investigations raises serious ethical and legal implications that must be reflected both in the guidelines given to law enforcement and in the policies that govern submission, removal, and retention of the information. Any U.S. system that facilitates international DNA sharing should address the concerns of the *Marper* court as well as incorporate traditional U.S. notions of privacy and liberty interests.

When Alec Jeffreys first conceived the idea of using DNA profiling to assist in criminal investigations, it is unlikely that he perceived the rapid growth in forensic science that would follow. Since that time, numerous countries have established DNA databases to both implicate and exonerate suspects, and the United Kingdom has taken the lead on exploring the potential for an enormous database. Recognizing the potential for using DNA databases to solve crimes and to prevent future crimes, England and Wales attempted to greatly expand its DNA database by allowing for the collection and indefinite retention of DNA profiles from arrestees. Since the 2008 ruling of the European Court of Human Rights, the United Kingdom has been forced to reevaluate their expansive policies and the implications of the *Marper* decision extending beyond an official mandate to revise policy. The decision has generated increased distrust among the public in the United Kingdom and has contributed to the undermining of what was an admirable effort to reduce crime and provide relief to families by utilizing DNA evidence to solve previously unsolvable cases.

As federal and state legislation in the United States become increasingly expansive, legislators and law enforcement need to be reminded that just because they have the technology to do something

does not mean they should do it. The *Marper* decision demonstrates how abuse of DNA technologies can lead to both a public and a judicial backlash. This Note proposes that the United States curb its collection and retention of DNA samples from arrestees, particularly in light of the presumption of innocence and the implications and stigma that necessarily result from telling innocent individuals that they have fewer rights because they have been arrested.

*Erica Solange Deray**

* J.D. Candidate 2011, Vanderbilt University Law School; B.A. 2006, Swarthmore College. The author would like to thank the editors and staff of the *Vanderbilt Journal of Transnational Law*, and all the friends who offered their advice and support along the way.
