

5-1-2013

Compulsory Collection and Retention of DNA Upon Arrest: Fourth Amendment Implications

Alyssa Mandara

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

Recommended Citation

Mandara, Alyssa, "Compulsory Collection and Retention of DNA Upon Arrest: Fourth Amendment Implications" (2013). *Law School Student Scholarship*. 160.

https://scholarship.shu.edu/student_scholarship/160

Alyssa Mandara
Compulsory Collection and Retention of DNA Upon Arrest: Fourth Amendment Implications

Table of Contents

I. INTRODUCTION..... 3
 The Problem: Compulsory Collection and Retention of DNA Upon Arrest..... 3
 DNA Databases..... 4

II. Current DNA Collection and Retention Policies..... 5

The United States 5
 DNA Retention and the Fourth Amendment..... 11
 DNA Collection Has No Fifth Amendment Implications 13
 Current Status of the DNA Act in the US..... 14

Council Of Europe Member States 15
 Introduction 15
 The United Kingdom..... 17
 Scotland..... 21
 Austria 28
 Belgium 29
 Bulgaria 29
 Cyprus..... 30
 Denmark 30
 Finland..... 31
 Germany..... 31

North and East Africa and the Middle East 33

China..... 33

Canada 34

III. Comparison and Recommendations 36
 Comparison of Compulsory DNA Collection..... 36
 Comparison of DNA Profile Retention..... 40

FINAL CONCLUSION 43

I. INTRODUCTION

The Problem: Compulsory Collection and Retention of DNA Upon Arrest

The following scenario, though a hypothetical, could be happening all over the United States because of the current DNA Act. John is arrested by the township police department on a burglary charge. Upon arrest, the police obtain a sample of John's DNA using a buccal swab. John does not give his consent for the sample nor do police obtain a warrant from the local magistrate. The charges against John are later dropped. John's DNA profile is entered into the local DNA database and also entered into CODIS, the federal DNA database. John is unaware his DNA was kept. He never writes to have his profile expunged from the record. A few years later there is a murder in John's town. Federal officials are called in to investigate the murder. The federal agents obtain DNA from the crime scene. The DNA sample is entered into the national database and alerts officials that John's sample is a partial match. Officials now know that the person who committed the murder is a male relative of John. Police go to John's town and use the partial match as probable cause to arrest all of John's male relatives in the area. Using the authority of the federal DNA Act, the federal agents obtain compulsory DNA samples of all the male relatives upon their arrest for the murder. John's cousin, Mark, is a direct match. Mark is charged with the murder.¹

Some people may read the preceding hypothetical and think, "Great, police were able to solve that murder." But others will read that scenario and shudder

¹ *DNA and Law Enforcement*; Karen J. Maschke; 2-3; published by the Hastings Center

because the DNA Act and the compulsory collection and retention of DNA from arrested individuals bypasses the protections of the Fourth Amendment and reeks of an unconstitutional search and seizure.

DNA Databases

The United States currently has the largest DNA database in the world.² Until a few years ago, the United Kingdom had the largest. As of 2012, 53 countries have established DNA databases.³ Six countries have enacted legislation establishing DNA databases.⁴ Three countries are considering legislation to establish DNA databases. Thirty-five countries are in the process of planning DNA databases.⁵ The United Arab Emirates is in the process of putting the entire population into a DNA database.⁶ In 2008, Uzbekistan declared it would put its entire population into a DNA database.⁷ US intelligence is currently building DNA databases in Afghanistan and Iraq.⁸ Bermuda has been entering DNA profiles into its national database since 2005, including the profiles of innocent people.⁹ In Argentina, families whose children went missing during the dictatorship have been voluntarily giving DNA samples to the national database.¹⁰ Based on the statistics, it is clear that DNA profiling is here to stay.

² Gene Watch UK; www.genewatch.org

³ Id.

⁴ Id.

⁵ Id.

⁶ Id.

⁷ Id.

⁸ Id.

⁹ Id.

¹⁰ Id.

II. Current DNA Collection and Retention Policies

The United States

DNA profiling has become so popular because it is a simple and accurate method for identification. In the United States, DNA profiling was first used to convict a criminal defendant in 1987 when forensic scientist recovered a DNA sample from a Florida rape victim to the DNA of the suspect.¹¹

Congress passed the DNA Analysis Backlog Elimination Act, 42 U.S.C.A. § 14135 in 2000. The statute authorized federal officials to collect DNA samples from people convicted of specific violent crimes who were in federal custody, including probationers, parolees, and people on supervised release. In 2004 Congress passed the Justice for All Act, which expanded DNA collection to any person convicted of any federal felony. Congress further expanded DNA legislation with the passage of the Violence Against Women Act of 2006 and the Adam Walsh Protection and Safety Act of 2006. These acts permit federal officials to obtain DNA from any person arrested for a federal felony and federal detainees who are neither US citizens nor permanent resident aliens.¹²

¹¹ *Questions of Time, Place, and Mo(o)re: Personal Property Rights and Continued Seizure Under the DNA Act*, Natalie Logan; page 2

¹² *DNA and Law Enforcement*; Karen J. Maschke; 2-3; published by the Hastings Center

On July 27, 2006 the new amendments to 42 U.S.C.A. § 14135a became effective.¹³ The amendments authorized DNA samples to be collected “from individuals who are arrested, facing charges, or convicted or from non-United States persons who are detained under the authority of the United States.”¹⁴ The statute states that “any felony” is any qualifying federal offense for purposes of the Act.¹⁵ The Act proscribes a criminal penalty for individuals who fail to cooperate in the collection of samples – failure to comply will result in the individual being guilty of a Class A misdemeanor and punished in accordance with Title 18.¹⁶

The DNA Act requires the Attorney General, the Director of the Bureau of Prisons, or the corresponding probation office to give every DNA sample taken pursuant to (a) to the Director of the FBI. The FBI will then analyze each sample and create a DNA profile.¹⁷ State and federal agencies submit locally analyzed DNA profiles to the National DNA Index System (NDIS). The FBI uses its software program, the Combined DNA Index System (CODIS) to link the profiles already contained in the state and federal databases.¹⁸

There are safeguards built into the statute and government policies that protect the genetic information and limit the reach of the Act. First, the Act requires the Director of the FBI to expunge the DNA record from CODIS when a conviction is overturned or when, if the sample is taken following an arrest, the charge is

¹³ 42 U.S.C.A. § 14135(a)

¹⁴ 42 U.S.C.A. § 14135(a)(1)(A)

¹⁵ 42 U.S.C.A. § 14135(d)(1)

¹⁶ 42 U.S.C.A. § 14135(a)(5)(A) and (B)

¹⁷ 42 U.S.C.A. § 14135(b)

¹⁸ *Questions of Time, Place, and Mo(o)re: Personal Property Rights and Continued Seizure Under the DNA Act*, Natalie Logan; page 3

dismissed or results in an acquittal or no charge is timely filed.¹⁹ In order for the FBI to expunge the record, the individual must send a certified copy of the final court order establishing the final disposition of the arrest or conviction.²⁰

There are two additional government policies that are not explicitly part of the statute but are important in protecting against the misuse of information. First, there are no names or other personal identifiers stored in CODIS. The database contains only the DNA profile, a number identifying the agency that submitted the DNA profile, a “Specimen Identification Number” (a number the FBI assigned sequentially at the time the sample is collected that does not correspond in any way to the individual’s social security number, criminal history identifier, or correctional facility identifier), and information identifying the laboratory personnel associated with creating the profile.²¹ The end result is that a CODIS user can only access a very limited amount of data, none of which can be used to identify the source of the DNA profile.²²

Second, the FBI has established a policy of using only “junk DNA.” Junk DNA refers to “non-genic stretches of DNA not presently recognized as being responsible for trait coding.”²³ The strict practice of analyzing and storing only “junk DNA”

¹⁹ 42 U.S.C.A. § 14135

²⁰ United States v. Mitchell, 652 F.3d 387 (3rd Cir. 2011); 42 U.S.C.A. § 14135(d)(1)(A)

²¹ <http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet>

²² United States v. Mitchell, 652 F.3d 387 (3rd Cir. 2011)

²³ United States v. Kincade, 379 F.3d 813, 818 (9th Cir. 2004) (en banc) (plurality opinion)

guarantees that important personal genetic information that reveals physical characteristics and medical conditions is not stored in CODIS.²⁴

Compulsory DNA Collection and the Fourth Amendment

The Fourth Amendment to the United States Constitution guarantees “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.”²⁵ A Fourth Amendment search occurs when the government infringes upon an expectation of privacy that society is prepared to consider reasonable.²⁶ “It is undisputed that a compelled DNA extraction is a “search” for Fourth Amendment purposes.”²⁷ “The compulsory extraction of blood for DNA profiling unquestionably implicates the right to personal security embodied in the Fourth Amendment, and thus constitutes a “search” within the meaning of the Constitution.”²⁸

Compulsory DNA collection pursuant to the Act implicates the Fourth Amendment in three different ways.²⁹ First, the collection of the sample is a search of the person.³⁰ Law enforcement can take DNA by using a blood sample or buccal swab of the interior of the individual’s cheek.³¹ Although this is a minimal intrusion, the Supreme Court has recognized that even minimal intrusions implicate the

²⁴ United States v. Mitchell, at 400

²⁵ U.S.C.A. Const.Amend. 4

²⁶ U.S.C.A. Const.Amend. 4

²⁷ Haskell v. Harris, 669 F.3d 1049 (9th Cir. 2012)

²⁸ United States v. Kincade, 379 F.3d 813, 821 (9th Cir. 2004) (en banc)

²⁹ Skinner v. Ry. Labor Execs.’ Ass’n, 489 U.S. 602, 612 (1989)

³⁰ Id.

³¹ Boroian v. Mueller, 616 F.3d 60 (1st Cir. 2010)

Fourth Amendment.³² Second, the collection of the sample is a seizure of the individual's bodily tissues.³³ Third, the analysis of the sample is a second, separate search.³⁴ The federal Circuit Courts have "unanimously upheld the analysis of DNA samples as searches for Fourth Amendment purposes" but have declined to find the analysis unreasonable.³⁵

Currently, the majority of United States Circuit Courts views the collection of DNA as parallel to the collection of a fingerprint and have held the compulsory collection and retention of DNA upon arrest does not violate the Fourth Amendment. The majority view is to analyze the constitutionality of the Act using a reasonableness approach: whether the intrusion is reasonable.³⁶ The courts apply a totality of circumstances test, "balancing the intrusion on an arrestee's privacy against the Government's interest in the collection and testing of his DNA."³⁷ For example, in Mitchell, the Third Circuit weighed the minimal intrusion of the buccal swab combined with an arrestee's diminished expectation of privacy in his identity against "the protections built into the Act, the Government's stated practice of only analyzing 'junk DNA', the current limits of technology, the information stored served only an identification purpose, the DNA served important law enforcement interests which were not equally well served by collecting DNA samples post conviction" and

³² Terry v. Ohio, 392 U.S. 1, 24-25 (1989)

³³ United States v. Kincade, 379 F.3d 813, 873 (9th Cir. 2004)

³⁴ Skinner v. United States, 489 U.S. 109 S.Ct. 1402, 616 (1989)

³⁵ Logan, page 12

³⁶ Haskell v. Harris (9th Cir.) (Analyzing CA statute comparable to DNA Act); United States v. Mitchell, 652 F.3d 387 (3rd Cir. 2011)

³⁷ United States v. Mitchell, 652 F.3d 387

determined the intrusion was reasonable and therefore not a violation of the Fourth Amendment.³⁸

The FBI's policy of using only "junk DNA" ensures that the CODIS DNA profiles can only be used for identification. In Mitchell, the Third Circuit found "the use of "junk DNA" creates a "DNA fingerprint" that yields precise information about identity but little or no other personal information."³⁹ The D.C. Circuit Court determined that because junk DNA is useful for only identification purposes, "CODIS functions much like an old-fashioned fingerprint database (albeit more efficiently)."⁴⁰ See also Boroian v. Mueller, 616 F.3d 60, 66-67 (1st Cir. 2010), stating that, "Given the DNA Act's stringent limitations on the creation and use of DNA profiles, CODIS currently functions much like a traditional fingerprint database, permitting law enforcement to match one identification record against others contained in the database."⁴¹ Both the Second and Tenth Circuits also determined the DNA Act's restrictions and FBI's use of junk DNA in CODIS permit the government to use a suspect's DNA in essentially the same way the government uses fingerprints and photographs to identify suspects and solve past and future crimes.⁴² Because courts view DNA profiles as analogous to fingerprint records, courts treat the intrusion of privacy under the DNA Act to be similar to the intrusion caused by the retention of fingerprint records.⁴³

³⁸ Id.

³⁹ United States v. Mitchell, at 401

⁴⁰ Johnson v. Quander, 440 F.3d 489, 499 (D.C.Cir.2006)

⁴¹ Boroian v. Mueller, 616 F.3d 60, 66-67 (1st Cir. 2010)

⁴² Banks v. United States, 490 F.3d 1178, 1192 (10th Cir.2007)

⁴³ Nicholas v. Goord, 430 F.3d 652, 671 (2d Cir.2005)

DNA Retention and the Fourth Amendment

DNA Retention Not an Unreasonable Search

Currently, the United States Supreme Court has not faced the question as to whether the retention of DNA samples or profiles is a constitutional violation. Boroian v. Mueller, a First Circuit decision, was the first decision regarding the government's retention of the sample in CODIS.⁴⁴ In Boroian, the First Circuit held the government's retention of Boroian's (a former probationer) blood sample and DNA profile pursuant to the DNA Act did not constitute a separate "search" in violation of the Fourth Amendment. The Court based its decision on the fact that the matching process used by CODIS was not a new search because it was limited to a comparison of the identification records already in the government's lawful possession. Furthermore, subsequent CODIS searches for matches did not reveal any new private information about Boroian or intrude in any way on his reasonable expectations of privacy. Therefore, the subsequent searches were not treated as new "searches" for Fourth Amendment purposes.⁴⁵

The federal courts' treatment of DNA profiles as analogous to fingerprints (for identification purposes only) lead the First Circuit to determine that DNA profiles fall under the 28 U.S.C. § 534(a), which requires the Attorney General to "acquire, collect, classify, and preserve" criminal identification records.⁴⁶ The government is not required to expunge the records, except for in very limited circumstances. ("It is

⁴⁴ *Questions of Time, Place, and Mo(o)re: Personal Property Rights and Continued Seizure Under the DNA Act*; Natalie Logan, 2012, Trustees of Boston University; Boroian v. Mueller, 616 F.3d 60 (1st Cir.)

⁴⁵ Id.

⁴⁶ Boroian v. Mueller, 616 F.3d at 67

well established that the state need not destroy records of identification – such as fingerprints, photographs, etc. – of convicted felons, once their sentences are up.”)⁴⁷

DNA Retention: Question of Continued Seizure

Boroian’s claim, that the retention of his DNA sample was an unreasonable search, failed.⁴⁸ However, on his appeal to the First Circuit, Boroian attempted to raise the allegation that the DNA Act was unconstitutional because it constituted a continued seizure, and was thus an unreasonable search.⁴⁹ The United States Supreme Court recognized the doctrine of continuing seizure in United States v. Place. The Court determined that a seizure of personal property could be reasonable on the onset but the continuing seizure could become unreasonable because of the length of time the property was held for.⁵⁰ However, when Boroian’s case reach the First Circuit on appeal, the Court refused to address the new complaint because Boroian had failed to raise the issue on his appeal to the lower court.⁵¹

The Continuous Seizure Doctrine is relevant to the DNA Act because it raises the important (and as yet unanswered question) of whether a person retains a possessory interest in his DNA after it has been taken by the government, profile, and entered into CODIS to be used in future DNA searches.⁵² The Supreme Court has not addressed the question of whether a person retains a possessory interest in

⁴⁷ United States v. Amerson, 483 F.3d 73, 86 (2d Cir. 2007)

⁴⁸ Boroian v. Mueller, 616 F.3d 60

⁴⁹ Boroian v. Mueller, *supra*

⁵⁰ United States v. Place, 462 U.S. 696, 697, 103 S. Ct. 2637, 2639, 77 L.Ed. 2d 110 (1983)

⁵¹ Boroian v. Mueller, *supra*

⁵² Logan, page 748 - 749

his DNA sample once it has been collected.⁵³ However, the leading state court case in possessory rights of biological matter, Moore v. Regents of the University of California, held that a person does not retain a property right in human tissue and biological matter that has been removed from his body.⁵⁴ Based on this decision, as well as the current trend in treating DNA samples and profiles on CODIS as comparable to a fingerprint database, my guess would be there would be no claim for maintaining a possessory interest in the blood or buccal swab that was removed from the body and used to create the DNA profile.

DNA Collection Has No Fifth Amendment Implications

The Fifth Amendment to the United States Constitution guarantees a person will not “be compelled in any criminal case to be a witness against himself.”⁵⁵ The compulsory collection of DNA samples does not implicate the Fifth Amendment. When a person is compelled to give a DNA sample, the sample is collected either through blood or a buccal swab of the inner cheek of the suspect (to collect saliva).

In Schmerber v. California, the Supreme Court ruled that physical characteristics are not subject to the self-incrimination clause and therefore the compulsory taking of the defendant’s blood was not a violation of the Fifth Amendment.⁵⁶ The Court has developed this concept over the years and ruled there are a number of situations where defendants and suspects are forced to provide physical information and there is no Fifth Amendment violation. See Pennsylvania v. Muniz, holding defendant’s answers to officers’ questions pursuant to a DUI stop

⁵³ Logan, page 749

⁵⁴ Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 480 (Cal. 1990)

⁵⁵ U.S.C.A. Const.Amend. 5

⁵⁶ Schmerber v. California, 384 U.D. 757, 86 S. Ct. 1826, 16 L. Ed. 2d 908 (1966)

prior to being given his Miranda warnings were admissible because slurred speech was a physical characteristic of the defendant and not “testimonial” and therefore not protected by the Fifth Amendment.⁵⁷ See also Gilbert v. California, holding a mere handwriting sample (as opposed to the content of what is written), is like the voice or body itself, an identifying physical characteristic, and not subject to constitutional protection.⁵⁸ Based on the case law, the DNA Act relates to physical characteristics and therefore is entirely constitutional under the Fifth Amendment.

Current Status of the DNA Act in the US

Every United States Circuit Court that has addressed the constitutionality of the DNA Act as applied to arrestees not yet convicted has upheld the Act as constitutional. However, on April 24, 2012 the Maryland Court of Appeals overturned the 2010 conviction and life sentence of Alonzo Jay King. King had been arrested for an assault in 2009. Upon his arrest, authorities took a DNA sample pursuant to a Maryland state law permitting police to obtain DNA samples from people arrested for violent crimes, attempted violent crimes, burglary, and attempted burglary. The DNA sample linked King to a rape that had gone unsolved for seven years. The Maryland Court of Appeals held Maryland’s DNA Collection Act was a violation to the Fourth Amendment because it constituted an unreasonable search and seizure.⁵⁹

Maryland applied for certiorari to the United States Supreme Court. On November 9, 2012 the High Court granted certiorari to determine whether a state

⁵⁷ Pennsylvania v. Muniz, 496 U.S. 582, 110 S. Ct. 2638, 110 L. Ed. 2d 528 (1990)

⁵⁸ Gilbert v. California, 388 U.S. 263, 87 S. Ct. 1951, 18 L. Ed. 2d 1178 (1967)

⁵⁹ “*Supreme Court Takes Up DNA and Sentencing Cases*” MSNBC; 11/09/2012; http://www.msnbc.msn.com/id/49765575/ns/us_news

may collect DNA samples from arrestees not yet convicted of violent crimes. Chief Justice Roberts noted the Maryland Court's decision conflicts with three other appellate courts that upheld DNA laws similar to Maryland's. Roberts said Maryland's decision "had national implications" because if the Maryland decision was upheld the FBI could not get Maryland arrestees' samples for CODIS.⁶⁰

Council Of Europe Member States

Introduction

The United Kingdom was the first European country to establish a national DNA database. Currently, most of the Council of Europe member States have established databases and permit the compulsory collection of DNA in the criminal context. Twenty-five States have provisions permitting the collection of DNA samples to be stored as a profile on a DNA database (Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain, and Sweden).⁶¹

DNA policies in the member States vary. Most countries do not permit automatic DNA collection in criminal proceedings but restrict sampling and profiling to specific circumstances, such as arrests for serious offenses or crimes punishable by certain prison terms (Austria, Belgium, Finland, France, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Spain, and Sweden).⁶² Five

⁶⁰ Id.

⁶¹ Gene Watch UK; Summary by Region: Europe; <http://www.genewatch.org/sub-568625>; accessed 10/26/2012

⁶² <http://www.statewatch.org/news/2008/dec/echr-marper-judgments.pdf>

countries (Belgium, Hungary, Ireland, Italy and Sweden) permit DNA samples to be obtained and profiles entered into the national database but require that the information be destroyed pursuant to a government order if the person is acquitted or criminal proceedings are not pursued.⁶³

Some countries permit retention for a limited time or for limited purposes. For example, Austria and Poland allow DNA profiles to be kept if there is a real risk the individual will commit a future dangerous offense.⁶⁴ Germany, Luxembourg, and the Netherlands authorize retention if the police continue to suspect the person or if the person is implicated in a separate criminal investigation.⁶⁵ While the UK is the only member State that once permitted indefinite retention, France has a very expansive retention policy: profiles can be kept for 25 years after the person is acquitted or charges dismissed.⁶⁶ However, during the retention period the prosecutor can order the profile be deleted (either on his own or upon request) if the DNA is no longer required for identification in a criminal prosecution.⁶⁷ Finland permits retention for one year after a person is acquittal.⁶⁸ Denmark law authorizes profile retention for 10 years after an acquittal.⁶⁹ Switzerland permits DNA to be kept for 1 year after criminal proceedings are discontinued.⁷⁰

⁶³ <http://www.statewatch.org/news/2008/dec/echr-marper-judgments.pdf>

⁶⁴ Id.

⁶⁵ Id.

⁶⁶ Id.

⁶⁷ Id.

⁶⁸ Id.

⁶⁹ Id.

⁷⁰ Id.

Italy has a very restrictive DNA policy. In June 2009 Italy passed legislation establishing a database for convicted offenders only. To obtain a DNA sample from a suspect, a judge must request the person's profile.⁷¹

The United Kingdom

Until recently, the United Kingdom had the largest DNA database in the world. The database, officially titled the UK National Criminal Intelligence DNA Database (NDNAD), was established in 1995. By March 2012 the database contained about 5,950,612 individual profiles. Approximately 30,000 new profiles are added to the database each month. The DNA samples are taken from crime scenes, police suspects, and, in England and Wales, from anyone arrested and detained at a police station. The current database has matched 400,000 crime scene DNA samples.⁷²

The main reason the UK database is so large is because once a profile is entered into the database it cannot be removed, even if the person is acquitted or the charges dropped.⁷³ As of 2004, any person arrested in England and Wales for any recordable offense (regardless of their age) has their DNA taken. The profile remains in the database permanently; the nature of the offense, the age of the offender, and acquittal or conviction are irrelevant.⁷⁴ Currently, the database

⁷¹ Id.

⁷² BBC News: "Time Limits on Innocent DNA Data"; BBC News; May 7, 2009; http://news.bbc.co.uk/2/hi/uk_news/8037042.stm

⁷³ BBC News: "All UK Must Be On Database"; published 2007/09/05; accessed 10/01/12; from BBC News: http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/6979138.stm; copyright BBC 2012

⁷⁴ Id.

contains 24,000 profiles of people aged 10-17 who were arrested and charged but never convicted of a crime.⁷⁵

The Data Protection Act of 1998

On October 24, 1995 the European Convention on Human Rights issued Directive 95/46/EC. The Directive's purpose was to protect the privacy of individuals (under Article 8 of the European Convention on Human Rights) by restricting the processing of individual personal data and limit the sharing of that data. The Directive enumerates policies and principles to restrict the processing and use of personal data while permitting individual Member States to enact legislation to ensure personal data is used for the prevention, investigation, detection and prosecution of criminal offenses.⁷⁶

On July 16, 1998 the United Kingdom adopted the Data Protection Act to effectuate the purpose of the Council's Directive. The Act states that the processing of personal data ("data which relate to a living individual who can be identified) is subjected to eight data protection measures. The first principle requires that personal data "shall be processed fairly and lawfully."⁷⁷ Pursuant to the Act, personal data processed for the prevention or detection of crime is excluded from the first principle's requirements.⁷⁸ The fifth principle of the Act orders that personal data processed for any purpose or purposes should not be kept for longer

⁷⁵ Id.

⁷⁶ <http://www.statewatch.org/news/2008/dec/echr-marper-judgment.html>

⁷⁷ Id.

⁷⁸ Id.

than is necessary for that purpose. The Act makes it a criminal offense not to comply with the protective and restrictive measures contained therein.⁷⁹

England, Wales, and Northern Ireland

In England and Wales, the Justice and Public Order Act of 1994 authorizes the entry of DNA profiles of persons charged with any recordable offense or who are convicted of any such offense.⁸⁰ All DNA profiles collected from crime scenes are also stored in the NDNAD.⁸¹ The Police and Criminal Evidence Act of 1984 permitted officers to take “non-intimate” samples from suspects without permission from the individual (for example: hair shafts).⁸² The Justice and Public Order Act changed the definition of non-intimate samples to include buccal swabs, therefore greatly expanding police sampling powers.⁸³ The statute applies to both convicted offenders and persons arrested or charged with an offense. Additionally, officers are authorized to collect DNA samples from minors (who are at least 10 years old) and from mentally ill people.⁸⁴ The Act imposes no restrictions on the collection of samples from crime scenes.⁸⁵

The Criminal Justice and Police of Act of 2001 authorizes the government to indefinitely retain the DNA profiles of both suspects and arrestees and convicted offenders. DNA profiles of persons who are later acquitted or whose charges are

⁷⁹ *Id.*

⁸⁰ www.councilforresponsiblegenetics.org/dnadata/Countries/GB.html; “United Kingdom” accessed 11/07/12

⁸¹ *Id.*

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*

dropped are also kept indefinitely on the database. DNA profiles generated from samples obtained from crime scenes are stored until identified or a match is found.⁸⁶

The inability of persons to remove their DNA profiles from the UK database has sparked international criticism. Home Office Minister Tony McNulty defends the database, stating the database has assisted police in solving about 20,000 crimes a year.⁸⁷ McNulty also said that although there are currently no plans to introduce DNA collection and profiling for all UK citizens, “no one ever said never.”⁸⁸ Lord Justice Sedley, an experienced and respected appellate court judge in England, publicly criticized the system, stating, “We have a situation where if you happen to have been in the hands of the police then your DNA is on permanent record. If you haven’t, it isn’t.”⁸⁹ Chief Constable of Lincolnshire Police and Chairman of the DNA Board, Tony Lake, stated DNA profiles from those convicted or arrested for violent or sexual offenses should stay on the database for life, but he does not think that needs to be the process for minor offenses.⁹⁰

Management of the National UK DNA Database

Beginning in 1995 the Chief Scientist of the Forensic Science Service was responsible for management of the National DNA Database.⁹¹ In July of 2005 the management of the database was transferred to the Home Office, who then transferred custodianship to the National Policing Improvement Agency.⁹²

⁸⁶ Id.

⁸⁷ Id.

⁸⁸ Id.

⁸⁹ Id.

⁹⁰ Id.

⁹¹ Id.

⁹² Id.

Scotland

In Scotland, the Criminal Procedure Act of 1995 permits the entry of DNA profiles from those individuals arrested for any recordable offense or who are convicted of any such offense.⁹³ DNA profiles derived from samples collected from crime scenes are also stored in the national database.⁹⁴ A police officer may request or use reasonable force to obtain a buccal swab from any person arrested for any recordable offense.⁹⁵ Officers may also request or forcibly take samples from minors (at least 10 years old) or from mentally ill persons.⁹⁶ As in England, there are no restrictions on collecting DNA samples from crime scenes.⁹⁷ Convicted persons' DNA profiles are kept indefinitely on the database.⁹⁸ If an arrested person is acquitted or, as soon as the decision is made not to initiate or pursue criminal proceedings against an arrestee, the arrestee's sample must immediately be removed from the database.⁹⁹ Samples collected from crime scenes are retained until identified but are not stored in the database until an identification of the sample is made.¹⁰⁰

Scotland's government may develop its own policies and procedures regarding the collection, treatment, and retention of DNA samples and profiles. However, Scotland's DNA database is not completely separate from England's and

⁹³ Id.

⁹⁴ Id.

⁹⁵ Id.

⁹⁶ Id.

⁹⁷ Id.

⁹⁸ Id.

⁹⁹ Id.

¹⁰⁰ Id.

Wales's. Scotland sends all its profiles to the NDNAD, meaning the national UK database contains almost all of the UK profiles.¹⁰¹

Challenges to DNA Retention in the UK: S and Marper

The United Kingdom is a member nation of the Council of Europe and therefore is subject to the rights granted by Section 1, Article 8 of the European Convention of Human Rights.¹⁰² Section 8 guarantees that 1) "Everyone has the right to respect for his private and family life, his home and his correspondence", and 2) "There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."¹⁰³

On August 16, 2004, two British citizens, Mr. Michael Marper, and "S" (request made by applicant not to have his name disclosed was granted by the court) brought two separate applications against the United Kingdom of Great Britain and Northern Ireland alleging violations under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁰⁴ S had been arrested on January 19, 2001 at the age of 11 and charged with attempted robbery. His fingerprints and DNA sample were taken pursuant to the Police and Criminal

¹⁰¹ Id.

¹⁰² <http://www.hri.org/docs/ECHR50.html>; The Council of Europe; The European Convention on Human Rights

¹⁰³ Id.; Section 1, Article 8 of The European Convention on Human Rights

¹⁰⁴ S and Marper v. United Kingdom;

<http://www.statewatch.org/news/2008/dec/echr-marper-judgement.pdf>

Evidence Act. On June 14, 2001 S was acquitted of the crime but his DNA profile remained on the UK national database.

Mr. Marper was arrested on March 13, 2001 and charged with harassment. At the time of his arrest his DNA and fingerprints were taken. No charges were ever pressed and criminal proceedings were never initiated.¹⁰⁵ His DNA profile remained on the database.

Both S and Marper asked for their fingerprints and DNA to be destroyed but police refused in both cases. S and Marper applied for judicial review of the officers' decisions not to destroy the samples. On March 22, 2012, the Administrative Court denied the applications. S and Marper appealed the decision to the Court of Appeal, which, on September 12, 2002, upheld the Administrative Court's decision. Lord Justice Walker (of the Court of Appeal) used a balancing test to determine whether the DNA samples should be retained. He found that the risks in keeping genetic material were outweighed by the benefits in achieving the UK's goals of prosecuting and preventing crime.¹⁰⁶

On July 22, 2004 the House of Lords dismissed an appeal brought by S and Marper. The House first noted past examples where a murderer and a rapist had either been acquitted of charges or a decision not to proceed with criminal proceedings had been made because DNA evidence linking the defendants to the crimes had not been able to be used. The House went on to cite a 1999 case where DNA evidence from "T" was used to link "T" to a rape, even though that DNA evidence should have been destroyed (under the earlier provisions of the Police and

¹⁰⁵ Id.

¹⁰⁶ Id.

Criminal Evidence Act). Additionally, the House referenced statistical evidence where 53 murders, 33 attempted murders, 94 rapes, 38 sexual offenses, 63 aggravated burglaries and 56 cases involving drug distribution were linked to DNA profiles that would have been destroyed under the earlier version of the Act.¹⁰⁷

In applying the balancing test, the House of Lords concluded that the retention of fingerprints and DNA samples did not constitute an interference with the right to respect for private life, but that even if there was an interference it was “modest indeed.”¹⁰⁸ The judges noted that the modest interference was justified by the purpose of retaining DNA profiles: the prevention of future crime and the right of other citizens to be free from crime.¹⁰⁹ In response to S’s and Marper’s argument that retention of their DNA profiles on the database without a conviction “created suspicion in respect of persons who had been acquitted”, the Home Secretary argued that retention of DNA “had nothing to do with the past” (the offense the person was acquitted for) but retention was to aid officers in their investigations of future crimes.¹¹⁰ The applicants, and other similarly situated, would only be impacted by the retention of their profiles if their profiles were a match for samples found at a future crime scene. The House of Lords determined retention of DNA profiles provided law enforcement with an enormous benefit and did not create a privacy intrusion under Article 8.¹¹¹

¹⁰⁷ Id.

¹⁰⁸ Id.

¹⁰⁹ Id.

¹¹⁰ Id.

¹¹¹ Id.

S and Marper brought their case before the European Court of Human Rights' Grand Chamber. Liberty and Privacy International, two non-governmental organizations, filed third-party briefs detailing the private nature of genetic material found in DNA samples. Liberty called attention to the important rights granted under the Convention: that government interference with an individual's rights must be "necessary in the democratic society" and have a legitimate goal of addressing a "pressing social need." Furthermore, the privacy interference must be in proportion to the goal and subject to the Court's review and approval.¹¹² S and Marper focused on the personal nature of the DNA samples along with their indefinite retention, stressing the data could be used to determine highly private information about medical conditions. They further claimed the retention had negative psychological implications because it exposed them to a certain negative criminal stigma.¹¹³

The UK government argued the Police and Criminal Evidence Act of 1984 authorized the collection of the samples and retention of the profiles. The government further alleged their activities did not fall within the purview of Article 8 because it was used only as a means of accurate identification and did not reveal any personal information about the individuals. The government stressed the important and legitimate goal of identifying future criminals as weighed against the minimal intrusion of collecting the samples.¹¹⁴

¹¹² Coster v. United Kingdom (2001) 33 EHRR 479

¹¹³ <http://www.statewatch.org/news/2008/dec/echr-marper-judgment.pdf>

¹¹⁴ Id.

The 17-judge bench unanimously ruled that the retention of the DNA samples in England, Wales, and Northern Ireland was a violation of Article 8 and awarded 42,000 pounds each to S and Marper. The Court stressed that the government interference with intimate details of individuals' personal information is of the utmost importance to the individual. The Court looked at how other Member States dealt with DNA collection and retention, focusing on Scotland. The Court determined that Scotland had developed a rational and proportionate method for the DNA issue: indefinite retention for convicted individuals, destruction of samples and profiles for those acquitted or whose charges were dropped. The judges decided that in dealing with issues such as this, where personal and important private information is at stake, Member States need to be given a narrow margin in how the individual states act. In this case, the Court declared that the United Kingdom was outside the margin and indefinite retention did not achieve the proper balance.¹¹⁵

United Kingdom Reaction to S and Marper

In May of 2009 the United Kingdom Home Office issued a declaration on how the UK would comply with the ruling of the European Court of Human Rights. According to the Court's decision, the 850,000 DNA profiles on the database should be removed because indefinite retention was a violation of Article 8. However, instead of removing the profiles the Home Office announced the following compliance measures:¹¹⁶

- The destruction of all original DNA samples as soon as a profile is created

¹¹⁵ *Id.*

¹¹⁶ "Time Limits on Innocent DNA Data";

http://news.bbc.co.uk/2/hi/uk_news/8037042.stm; May 7, 2009; BBC News

- After 12 years: Automatic deletion of profiles of those arrested for a violent or sexual crime but not convicted
- After six years: Automatic deletion of profiles of those arrested but not convicted
- Indefinite retention of DNA and fingerprints of anyone convicted of a recordable offense
- Removal of juvenile's profiles who were arrested but never convicted, or convicted of a minor offense, at the age of 18
- Removal of DNA profiles for all children under 10 (already achieved at the time of the ruling)
- Approximately 850,000 profiles are affected by the ruling and it would take up to two years to work through all the cases¹¹⁷

Advocacy groups for individual rights alleged the UK's compliance plan was an insult to the Court's ruling that the database (excluding Scotland) was a violation of Article 8. Government officials claimed the time limitations are enough to comply with the ruling but fear that with the cuts fewer crimes will be solved.¹¹⁸ Estimates range from 4500 fewer crimes being solved each year, with that number rising to 26,000 if the retention policies are extended to fingerprint retention, which is the current plan.¹¹⁹

Vernon Coaker, Home Office minister, stated that retention of DNA is a vital tool in solving future crimes because, according to current research, half of the individuals arrested and convicted reoffend within six years and two-thirds reoffend within 12 years. Because of the recidivism rates, the DNA stored on the database is essential to matching potential samples to individuals. Jill Saward, crime victim advocate, stated removing all the records from the database would contribute to an "ongoing erosion of justice" in the United Kingdom.¹²⁰

¹¹⁷ Id.

¹¹⁸ Id.

¹¹⁹ Id.

¹²⁰ Id.

Jacqui Smith, UK Home Secretary, stated the government's proposed measures would guarantee those should remain on the database would, while establishing a time for removal for those who should be removed.¹²¹ Not all government officials agreed with the government's proposal. Chris Gayling, shadow home secretary, stated the government should adopt the Scottish model, which had been praised by the European Court of Human Rights. Gayling said, "People in Britain should be innocent until proven guilty."¹²² Gayling went on to allege the ministers were trying to do as little as possible and the new measures were "just not good enough."¹²³ Government Democrats and liberals think DNA should be taken upon arrest but if the person is cleared the information should not be retained at all.¹²⁴ For now, the current policies will remain in effect.

Austria

Austria established its DNA database in 1997. At the time of the 2008 Interpol survey, the database contained 32,000 crime scene profiles, 117,150 individual profiles, 103 missing person profiles, and 61 profiles from unknown or deceased persons. The database is run by the Ministry of the Interior. In Austria, DNA is taken only from convicted offenders and persons suspected of serious offenses. Profiles may be deleted and samples destroyed upon acquittal, but only on written application.¹²⁵

¹²¹ Id.

¹²² Id.

¹²³ Id.

¹²⁴ Id.

¹²⁵ Id.

Belgium

In Belgium, DNA is taken without suspects' consent when the person is suspected of committing a crime with a prison sentence of five or more years. DNA can also be taken without permission upon order of a magistrate, based on crime scene evidence. DNA profiles of individuals convicted of serious offenses (mostly rape and murder) are retained indefinitely on the database. However, all physical DNA samples must be destroyed once profiles are obtained. At the time of the 2008 Interpol survey, the Belgium database contained 14,000 crime scene profiles and 14,000 individual profiles.¹²⁶

Bulgaria

The Bulgarian DNA database was established in 1999. Police may take DNA from suspects in criminal cases, for crime prevention, or from persons who are a threat to national security. Profiles taken for national security reasons or crime prevention must be erased if there is no reason for retaining the information. The Ministry of the Interior determines whether or not a profile should be retained or deleted. In determining retention, the Ministry considers the age of the information, the need for the information for the completion of an ongoing investigation, whether the person has a prior conviction, or the expiration of the term for retention as provided by law. Profiles taken for reasons other than for crime prevention may only be deleted upon written order of the Data Commissioner or upon a written request from the individual. Additionally, to be deleted, the profile must have either been registered unlawfully, the individual was acquitted, the individual is exempt because of incapacity, or the person is deceased. At the time of the 2008 Interpol

¹²⁶ Id.

survey, the Bulgarian database contained 940 crime scene profiles, 16,100 individual profiles, and 15 profiles from unknown/deceased persons.¹²⁷

Cyprus

The Cyprus DNA database was established in 1998. Cyprus has new legislation planned, but the database is currently operating under the Police Law and Protection of Personal Data Act. The Cyprus Police Headquarters, the Laboratory of Forensic Genetics, and the Cyprus Institute of Neurology and Genetics operate and maintain the DNA database. Police may only obtain a DNA sample from a suspect upon a written court order. If the court does not issue an order then the police need the suspect's written permission. Convicted persons' profiles are retained indefinitely unless their record is expunged. Suspects' profiles are removed upon acquittal or upon clearance of charges. Crime scene stains are retained until identified. In 2008, Cyprus reported to the Interpol survey 1300 crime scene profiles, 520 individual profiles, 1590 missing persons' profiles, and five profiles from unknown or deceased individuals.¹²⁸

Denmark

Denmark created its DNA database in 2000 under the Law Establishing a Central DNA Profile Register. Under the law, police can take samples from a convicted person, a suspect charged with a crime that could lead to a prison term of one and a half years or more, and all crime scene stains. After the Court's decision in Marper, Denmark amended its DNA retention policies. After the ruling, innocent persons' profiles, samples, and fingerprints may be retained for 10 years after an

¹²⁷ Id.

¹²⁸ Id.

acquittal. Convicted persons' and suspects' profiles are retained until two years after death or upon turning 80 years old.¹²⁹

Finland

Finland established its DNA database in 1999 pursuant to the Coercive Measures Act, the Police Act, and the Police Personal Data File Act. The law authorizes DNA collection from persons serving a prison sentence of three or more years, suspects charged with a crime that has a potential prison sentence of six months or more, and all crime scene stains. Convicted persons' profiles are retained for 10 years after death. Suspects' profiles are removed within one year of the prosecutor's determination there is no evidence, charges are dismissed, the sentence is nullified, or 10 years after the suspect's death (if the information was not removed earlier). Crime scene profiles are retained indefinitely. At the time of Interpol's 2008 survey, Finland's database contained 63,030 individual profiles and 9517 crime scene profiles.¹³⁰

Germany

In 1998, the German DNA database was established under the Rules of Legal Procedure, the Act for the Establishment of Identity, and the Act for the Federal Criminal Investigation Office. At the time of Interpol's 2008 survey, there were 132,252 crime scene profiles, 571,250 individual profiles, 972 missing person profiles, and 438 profiles from unknown or deceased persons on the database.¹³¹

¹²⁹ Id.

¹³⁰ Id.

¹³¹ Id.

Pursuant to the laws, DNA is collected from people convicted of a serious offense, people repeatedly committing the same minor offenses, suspects charged with a serious offense, and crime scene stains related to any recordable offense. The samples may be taken without the suspect's consent when the sample is necessary for an investigation and when the government has approval from a judge. If the delay caused by waiting for a judicial order would damage the investigation, the public prosecutor may issue the collection order. A judge may only order coercive sampling from a convicted person when the person is convicted of a serious or sexual offense and it is likely the person will recommit. Persons who repeatedly commit the same offenses are treated as having committed a serious offense. If the convicted person does not fit into the above categories, the person needs to give consent before DNA may be taken. Under the law, police are authorized to take samples from third party witnesses without consent if taking a sample is deemed necessary for establishing the truth.¹³²

Convicted persons' and suspects' profiles must be removed from the database when retention is no longer necessary. German law sets time frames in which the government must decide whether retention of profiles is necessary. For convicted adults, the government must decide whether retention is necessary within 10 years of sentencing; for minors, the government must decide within 5 years of sentencing. Crime scene profiles are deleted 30 years after their entry. Unidentified profiles must be removed after 30 years as well, although most are deleted after 10 years. Convicted persons' and suspects' physical samples must be

¹³² Id.

destroyed when they are no longer useful for investigation. Only unidentified DNA samples can be retained for further purposes.¹³³

North and East Africa and the Middle East

Many countries in Northern and Eastern Africa and the Middle East have already established DNA databases. Currently, there are active national databases in Bahrain, Egypt, Iran, Israel, Jordan, Kuwait, Morocco, Saudi Arabia, Tunisia, and the United Arab Emirates.¹³⁴ The policies and legislation behind the establishment of these nations' databases vary. For example, Israel may enact legislation to create a DNA database for missing persons and the United Arab Emirates is attempting to profile its entire population.

A the time of Interpol's 2008 survey, Algeria, Lebanon, Libya, Oman, Qatar, and Syria had initiated plans for establishing DNA profiles. According to Gene Watch UK, no further information is available, possibly due to last year's unrest in these regions.¹³⁵

China

The Chinese database was established in 2004. Currently, China has the third largest DNA database in the world, although only a small portion of the population is profiled and stored.¹³⁶ According to the 2008 Interpol survey, 126,000 crime scene

¹³³ Id.

¹³⁴ Id.

¹³⁵ Id.

¹³⁶ Id.

DNA profiles, 1,065,000 individual profiles, and 9600 unknown/deceased profiles were stored on the Chinese database. Hong Kong had its own separate database since 200, using the US CODIS system (4,161 crime scene profiles and 16,235 individual profiles).¹³⁷

The Chinese system does not operate like many of the other national databases in the world. The Chinese government targets certain segments of the population and then collects their DNA; DNA collection is not limited to those arrested or convicted of criminal offenses. In August of 2009 police in southern China began collecting and maintaining DNA records of employees working in nightclubs, bars and KTVs. According to a report by the Yangcheng Evening News, in order to keep their jobs, all employees in the entertainment industry would need a certificate showing they had their DNA, fingerprints, and handwriting collected by police. Long Shijun, deputy director of a police station in Guangzhou said the police were collecting and marinating this information to assist in monitoring entertainment venues, considered to be “hotbeds” of crime. Critics complained the policy proved a longstanding prejudice against people connected with the nighttime entertainment industry along with violating the legal principle of innocent until proven guilty.¹³⁸

Canada

On December 10, 1998 the Canadian government accepted the DNA Identification Act after years of pressure from the Canadian police community. The

¹³⁷ <http://www.genewatch.org/sub-566757>: China

¹³⁸ “Police Take Entertainment Workers’ DNA”; 08/13/2009; Web Editor: Jiang Aitao; <http://english.cri.cn/6909/2009/08/13/189s50856.htm>

Act amended the Canadian Criminal Code to allow judges to order people convicted of certain offenses to provide blood, buccal, or hair samples. In addition, the law created a national DNA database where convicts' DNA profiles, derived from the physical samples, would be stored. The Minister of Public Safety and Emergency Preparedness would be responsible for establishing the database. The law went into effect on June 30, 2000.¹³⁹

The official purpose of the Act is to “establish a national DNA data bank to help law enforcement agencies identify persons alleged to have committed designated offenses, including those committed before the coming into force of this Act.” The statute states that both the “protection of society and the administration of justice are well-served by the early detection, arrest and conviction of offenders, which can be facilitated by the use of DNA profiles.” The Act clearly stipulates that in order to protect individuals' privacy, DNA samples and profiles may only be used for law enforcement purposes and that safeguards must be placed on the use of DNA information along with access to the samples and data bank.¹⁴⁰

Under Canadian law, the profiles of convicted persons are to be retained indefinitely. However, the Act states that DNA samples and profiles are to be destroyed and removed “without delay” if a person is acquitted of the offense for which DNA was collected.¹⁴¹

¹³⁹ Royal Canadian mounted Police; www.rcmp.gc.ca; National DNA Data Bank

¹⁴⁰ DNA Identification Act S.C. 1998, c. 37 Assented to 1998-12-10

¹⁴¹ Id.

III. Comparison and Recommendations

Comparison of Compulsory DNA Collection

Most of the countries with DNA databases permit the compulsory collection of DNA upon the arrest of a suspect pursuant to the national DNA laws. For example, in the United States and United Kingdom, upon arrest law enforcement is authorized to take a DNA sample, generate a profile, and enter the profile into that country's national DNA database. Germany has a slightly stricter policy: German law requires a judicial order for a coerced sample, or, at the very least, authorization from the local prosecutor. Canada and Italy permit DNA samples to be taken only from convicted persons.

Compulsory DNA collection upon arrest has been most notably challenged in the United States as a violation of the Fourth Amendment's guarantee of unreasonable searches and seizures. However, no court to date has held the DNA law to be unconstitutional. Even the European Court of Human Rights did not find that the UK's collection law violated Article 8 of the Convention for Human Rights.

Currently the United States Supreme Court is considering the constitutionality of Maryland's DNA collection law as applied to arrestees.¹⁴² The Maryland Court of Appeals ruled the compulsory collection of suspects' and arrestees' DNA is unconstitutional.¹⁴³ Most likely, the US Supreme Court will agree with the Circuit Courts who have addressed the constitutionality of the federal DNA

¹⁴² Maryland v. King, 12-207, 2012 WL 3528106 (U.S. Nov. 9, 2012)

¹⁴³ King v. State, 425 Md. 550, 42 A.3d 549 (2012), reconsideration denied (May 18, 2012), cert. granted, 12-207, 2012 WL 3528106 (U.S. Nov. 9, 2012)

Act, and agree that compulsory collection of DNA at the time of arrest is constitutional and not an unreasonable search or seizure.

Opinion and Recommendations for DNA Collection Policies in the US

I do not think law enforcement should be permitted to take DNA upon arrest. This policy bypasses the Amendment's protections and puts innocent civilians at risk for profiling.

First, the primary justification given for DNA collection upon arrest is identification.¹⁴⁴ However, as the Maryland Court of Appeals noted in the King decision, once the suspect is identified through the routine booking and fingerprint process, the government no longer needs the DNA for identification.¹⁴⁵ In fact, the court adamantly stated "solving cold cases" was the only State interest served by the collection of King's DNA.¹⁴⁶ This means the DNA collection was a warrantless, suspicionless search conducted only for the "generalized interest" in solving crime. The United States Constitution and the Supreme Court mandate that "a warrantless, suspicionless search cannot be upheld by a 'generalized interest' in solving crimes."¹⁴⁷ Therefore, taking a suspect's DNA upon his arrest when that DNA is not needed to accurately identify him is a clear violation of the Fourth Amendment.

Second, compulsory collection pursuant to the federal DNA Act or state DNA laws is not the only way for law enforcement to obtain DNA samples and profiles.

¹⁴⁴ King v. State, 425 Md. 550, 42 A.3d 549 (2012), reconsideration denied (May 18, 2012), cert. granted, 12-207, 2012 WL 3528106 (U.S. Nov. 9, 2012)

¹⁴⁵ Id.

¹⁴⁶ Id.

¹⁴⁷ U.S.C.A. Const.Amend. 4; City of Indianapolis v. Edmond, 531 U.S. 32, 121 S. Ct. 447, 148 L. Ed. 2d 333 (2000)

Law enforcement can obtain a special DNA search warrant to obtain a DNA sample from a suspect.¹⁴⁸ The search warrant requires a showing of probable cause that the DNA sample will aid in the investigation (usually by connecting the suspect to the crime or by eliminating the person as a suspect). The warrant requirement upholds the values of the Fourth Amendment and ensures that law enforcement does not bypass the Constitution.¹⁴⁹

Congress and courts have permitted police officers and prosecutors to bypass the probable cause requirement of the Fourth Amendment by enacting and upholding the compulsory collection section of the DNA Act. The probable cause that forms the basis of the arrest is not always the same probable cause that justifies the taking of the DNA sample.¹⁵⁰ If officers had to obtain a DNA search warrant, they would need to establish probable cause that DNA will link the individual to the crime or be useful in the investigation for the crime the individual was arrested for.

For example, in King, the police did not collect King's DNA for the assault charge; it was collected pursuant to the Maryland law. The DNA was therefore not collected pursuant to the probable cause of the arrest but was taken only on the authority of the statute. The Maryland Court of Appeals stated, "Establishing probable cause to arrest a person is not, by itself, sufficient to permit a biological specimen to be taken from the person without first obtaining a search warrant." I agree. In my opinion, if police officers applied for a search warrant to obtain a DNA

¹⁴⁸ Winston v. Lee, 470 U.S. 753, 105 S. Ct. 1611, 84 L. Ed. 2d 662 (1985)

¹⁴⁹ Id.

¹⁵⁰ King v. State, 425 Md. 550, 42 A.3d 549 (2012), reconsideration denied (May 18, 2012), cert. granted, 12-207, 2012 WL 3528106 (U.S. Nov. 9, 2012)

sample from King for the assault charge they would not have met the probable cause requirement (especially since officers had already accurately identified King). The compulsory collection laws permit law enforcement to bypass the probable cause requirement when they collect DNA without a warrant because the probable cause for the arrest is not the same probable cause required to take the sample.

In my opinion, the biggest problem with permitting law enforcement to obtain a DNA sample from an arrestee without a warrant is the potential for profiling and abuse. Under the current law, a police officer could arrest someone who he considers “suspicious” for a minor felony offense as a pretext for obtaining a DNA sample, with the hope of running the profile through CODIS and connecting the arrestee to a different crime that there is no other strong evidence for. While this is definitely efficient, it is not constitutional and runs afoul of the entire adversarial system. Police and prosecutors are required to investigate and gather evidence pursuant to the protections put in place by the Constitution.

I recognize that popular opinion and case law are against me. The use of DNA for identification purposes has ensured that DNA collection upon arrest will continue in the United States. Additionally, courts have continuously bypassed the probable cause issue by finding that DNA profiling is only for identification, even though other courts, such as the House of Lords in the Marper case, and the Maryland Court of Appeals in King clearly noted stored DNA information is useful for the prevention of future crimes.¹⁵¹

¹⁵¹ See S and Marper and King, *supra*

Comparison of DNA Profile Retention

DNA profile retention policies vary around the world. Prior to the Marper decision, the United Kingdom had the broadest retention policy for non-convicted persons: DNA profiles from arrestees and suspects were retained indefinitely. The UK began the process of changing its retention policy when the European Court of Human Rights ruled (in Marper) the UK policy violated Article 8.

Other countries have stricter policies. Prior to Marper, Denmark had a broad retention policy. However, after the decision, Denmark amended its policy. Currently, innocent persons' profiles may be retained for 10 years after their acquittal or clearance of charges; after 10 years the records must be removed.¹⁵² Austria permits profiles to be deleted and samples to be destroyed upon acquittal if written application is made.¹⁵³ Cyprus permits convicted persons' profiles to be retained indefinitely but requires suspects' profiles be removed upon acquittal or clearance of the charges. The overall theme is that arrestees' samples cannot be retained indefinitely if they are never prosecuted and convicted of a crime.

The United States follows this approach. Convicted persons' profiles are retained indefinitely but arrestees' profiles must be removed if charges are not pursued or if there is an acquittal. However, in the US the cleared person is responsible for submitting a written request that his profile be deleted along with proof that charges were dropped or he was acquitted.

¹⁵² Gene Watch UK; <http://www.genewatch.org>; Denmark

¹⁵³ Gene Watch UK; <http://www.genewatch.org>; Austria

Opinion and Recommendations for DNA Retention Policies in the US

In my opinion, in this area of DNA retention, Scotland has achieved the correct balance. When charges are not pursued or a person is acquitted it is the responsibility of the government to remove the arrested person's DNA profile and sample. This approach adequately serves law enforcement's interest in identifying individuals upon arrest and using DNA to investigate crimes while protecting the privacy of innocent persons.

Convicted persons have a lesser expectation of privacy in their identity and therefore convicted persons give up rights upon their conviction.¹⁵⁴ Subsequently, retaining DNA profiles of convicted persons is in line with the Fourth Amendment.

An arrestee, on the other hand, is in a different category than a convicted person. An arrestee, through his arrest, does have a diminished expectation of privacy in his identity than someone who is not under arrest and identification is the main justification for taking a DNA sample upon arrest.¹⁵⁵ Additionally, the government has a legitimate interest in having an accurate and efficient tool (DNA) for investigating a crime.

However, once the person is accurately identified, if charges are later dropped or the person is acquitted of the charges, his status returns to that of a full citizen who has every expectation of privacy in his identity. Retaining DNA profiles of individuals when charges have been dropped or there has been an acquittal is a clear violation of the Fourth Amendment and an intrusion into a person's

¹⁵⁴ Griffin v. Wisconsin, 483 U.S. 868, 107 S. Ct. 3164, 97 L. Ed. 2d 709 (1987); United States v. Kincade, 345 F.3d 1095, 1113 (9th Cir. 2004)

¹⁵⁵ Id.

expectation of privacy in his identity. Furthermore, “the State interest in supervision and prevention of recidivism are much diminished, if not absent, in the context of arrestees and pretrial detainees.”¹⁵⁶

Retaining DNA of persons who have not been convicted also violates the presumption of innocence surrounding arrestees.¹⁵⁷ The government interest in storing DNA of persons who have not been convicted of a crime is not close to sufficient to overcome this historical and traditional presumption. Retaining DNA of an innocent persons stains that person’s presumption for any future arrest because immediately law enforcement has access to his profile and knows he was previously arrested.

Take Denmark as an example. Denmark’s policy of retaining innocent persons’ profiles for 10 years after acquittal or after charges have been dropped is a violation of the innocent person’s rights. Once the person is cleared, his life prior to his arrest should be returned to him. Retaining his DNA profile has changed his status under the law because now he is in a different position than a person who has never been convicted of a crime. His arrest, which never resulted in a conviction and could have been the result of any number of factors (mistake, illegal racial profiling), has now, in my opinion, impermissibly affected his future and changed his identification status. All non-convicted persons should be equal in their legal status, but an arrestee’s status is no longer equal and the arrest follows him into his future (10 years into his future in the case of Denmark).

¹⁵⁶ Mitchell, 652 F.3d at 415 n. 25 (quoting United States v. Scott, 450 F.3d 863, 874 (9th Cir.2006)

¹⁵⁷ King v. State, *Supra*

The United States has almost achieved the correct balance. However, I think that requiring an innocent person to submit a written request and proof of his innocence places too high a burden on that person. Once the person is cleared or charges are not pursued, the burden should be on the government, who arrested, charged, or convicted the person in the first place, to then set the record straight. All too often a person who is less educated or more poorly represented will not be aware that his DNA will be indefinitely retained unless he submits evidence of his clearance or acquittal and requests the deletion of his DNA profile. This has the potential to open the door to Due Process and Equal Protection Claims.

The bottom line is the person has been declared innocent, but because his records are retained, he is no longer on equal footing before the law as another innocent person has never been arrested. Arrests, without conviction, should not alter a person's status, disturb the presumption of innocence, and follow a person into his future.

FINAL CONCLUSION

DNA profiling is here to stay. Using DNA for identification and investigation in criminal matters is useful in solving crime but has serious implications on a person's rights under the Fourth Amendment. The best scenario would be to require a search warrant based on probable cause to obtain a DNA sample. If the person is convicted, his DNA profile should remain on the national database indefinitely. If charges are not pursued or the person is later acquitted, the burden

should be on the government to immediately remove the profile and destroy the sample. This policy achieves the correct balance between the government's legitimate interests in identification and investigation and an individual's rights under the Fourth Amendment.