COMPARISON OF DATA PROTECTION IN FORENSIC DNA DATABANKS IN CANADA AND THE UNITED KINGDOM

By Michelle Kisluk

Submitted to

Central European University
Department of Legal Studies

In partial fulfilment of the requirements for the degree of Master of Laws

Supervisor: Professor Judit Sándor

Budapest, Hungary

2008

Executive Summary

This paper examines the legal regimes governing forensic DNA databanks in Canada and the United Kingdom with respect to data protection. The question of which regime better protects forensic DNA data is examined through a comparison of the forensic DNA databank legal frameworks in Canada and the United Kingdom from the initial collection of DNA samples and permitted uses and disclosures through to their ultimate retention or destruction. Following the comparison of the two systems in this manner, data protection issues inherent in forensic DNA databank systems are examined through the framework of Canada and the United Kingdom's DNA databanks. These issues include: (i) the trend of expanding DNA databanks by broadening whose DNA is taken and retained; (ii) the potential for forensic DNA data to be used for secondary purposes (including in light of scientific development which permits the derivation of more information from a DNA sample); and (iii) the risk of loss or malfeasance. These risks and their implications on data protection are discussed and the two regimes compared with respect to how they deal with such issues.

Following the comparison of the two systems and discussion of general risks, this paper proposes recommendations for structuring a DNA databank regime in light of the research undertaken. A system is proposed which, amongst other suggestions, limits the number of people included in the DNA databank by limiting collection and retention practices. In conclusion, this paper finds that Canada's DNA databank framework is more data-protection-friendly than that of the United Kingdom based on a number of factors, including its laws regulating the conditions under which DNA may be taken, retained, used and shared.

Acknowledgements

The author would like to acknowledge the generous support of Central European University for a research grant to spend January – March, 2008 at the Center for Constitutional Studies and Democratic Development ("CCSDD") in Bologna, Italy conducting research for this paper. Also recognized is the support and hospitality of the CCSDD and, in particular, its director Justin Frosini. Finally, Professor Ian Kerr of the University of Ottawa, Enzo Rondinelli of DNA Netletter, Patricia Kosseim and Carman Baggarley of the Office of the Privacy Commissioner of Canada and Andre Savoie of Canada's National DNA Data Bank are thanked for generously providing their assistance and time. Finally, the author would like to thank Central European University and Professor Judit Sándor for supervising and reviewing this research.

Table of Contents

INTRODUCTION

Every day in the news and on television police shows, crimes are shown being solved and criminals taken off the streets through the use of DNA evidence. These stories tell of DNA found at a crime scene being matched against DNA already held by the police and the criminals are caught. The part of the story that the news and television shows do not tell, however, is what the other implications of having DNA held by the State are, and how different the same story could be depending on the country and the applicable legal framework in which the national forensic DNA databank[1] operates.

In what follows, this paper will examine the background to these police success stories and look at the laws determining whose DNA is stored and how having one's DNA in a forensic DNA databank may risk exposing personal information in ways beyond those necessary for forensic purposes and without the consent of the individual. This is a timely issue insofar as it is one often discussed in the media, public policy and academic journals, especially in today's post 9/11 anti-terrorism climate, when personal liberties are being often asked to make way for better security and investigative methods. It is an especially timely topic as in recent years many countries have been expanding their DNA databanks, often at the behest of tough-on-crime politicians and to the dismay of civil rights activists.

In this paper, the legal frameworks governing forensic DNA databank regimes in Canada and the United Kingdom will be examined, compared and analyzed. They represent two extremes of how national laws have dealt with the criminal justice and data protection issues that often conflict in the management of a DNA databank, with the United Kingdom at the extreme of including a wider scope of individuals in the DNA databank and Canada at the opposite extreme. While the United Kingdom's system is often referenced in literature on the

[1] Note that different countries use different terminology (e.g. Canada's "National DNA Data Bank" and the United Kingdom's "National DNA Database"). For the purposes of this paper, the generic term "DNA databank" will be used when referring to national DNA databanks/databases in general, and this paper will otherwise address specific national DNA databanks by their specific names.

topic of DNA databanks and privacy issues, there is not yet a comparison of it at this level of granularity to examine how its DNA databank regime measures in comparison to a country at the other extreme, in this case, Canada, in respect of data protection.

By looking at systems at both ends of the spectrum and, with insight from the existing literature on the subject, examining gaps in data protection, shared and those unique to one regime or the other, potential solutions are found and recommendations are made in Chapter 4. This paper concludes that in general the forensic DNA databank system in Canada respects data protection to a greater extent than in the United Kingdom and is better prepared in the event of technological and scientific changes which expand the potential information derivable from a DNA sample.

This chapter will provide an overview of the history, mechanics and implications of the use of DNA databanks in the forensic context, including a brief overview of how DNA matching works. This chapter will also highlight the importance of the protection of genetic data and it will outline the implications of data protection practices with respect to DNA samples. In Chapters 2 and 3, this paper will build on the background information provided in Chapter 1 and will examine the legal frameworks regulating Canada's and the United Kingdom's forensic DNA databanks with respect to whose information is stored, what that information includes and how its use and disclosure are regulated by law. In Chapter 4, potential data protection risks faced by the two regimes will be analyzed and recommendations proposed.

CHAPTER 1 –

BACKGROUND TO FORENSIC DNA DATABANKS AND DATA PROTECTION

1.1 The Rise of Forensic DNA Databanks

Since the 1980's, when DNA profiling techniques were being developed, the use of DNA evidence in the criminal process has become increasingly relied upon, as improvements in science and technology have increased the effectiveness and reliability of such evidence.[2] The predecessor to DNA evidence was the technique of fingerprint matching, which had been in practice since the 19th century.[3] The first conviction based on DNA profiling was a British case in 1986[4] in which crime scene stains at two murder scenes showed that the murderer in each case had the same blood type. This information, however, only permitted police to narrow the search down to a certain genetic property shared by 10% of people in Britain. Improvements in the technique a number of years after the murders permitted the DNA testing of the two crime scene stains against a blood sample of the prime suspect, proving that the two victims were murdered by the same person, but *not* by the man who had been the prime suspect.[5]

The police then conducted a "DNA dragnet", which is a sweeping collection of DNA of everyone in a particular target group, for example all males in a certain age range living within a certain vicinity. This particular DNA dragnet involved the collection of samples from over 5000 men from the region and DNA profiling was conducted on samples from the 10 percent who matched the blood type of the murderer. Ironically, in an early demonstration of the importance of the human factor in even the most cutting-edge scientific DNA profiling,

[2] Thomas J. Moyer, Chief Justice & Stephen P. Anwa, *Biotechnology and The Bar: A Response To The Growing Divide Between Science And The Legal Environment*, 22 Berkley Tech. L.J. 671 (2006) at 673 [hereinafter "Moyer"].
[3] See e.g. Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical Issues*, (September, 2007), available at: http://www.nuffieldbioethics.org/go/ourwork/bioinformationuse/introduction [hereinafter "Nuffield Report"] at s. 1.14.
[4] Forensic Science Service: *Casefile "Colin Pitchfork - first murder conviction on DNA evidence also clears the prime suspect"*, http://www.forensic.gov.uk/html/media/case-studies/f-18.html (last visited 10 October, 2008).
[5] *Id.*

the murderer was identified not through his participation in the DNA dragnet, but rather when a man was overheard saying that his friend had given a sample in his name. This comment triggered concern and eventually led to testing of the man's actual DNA, which showed a match to that of the murderer, and on this basis he was convicted.[6]

Since the time of Pitchfork's conviction, technological and scientific improvements, including the development of more accurate forensic DNA profiles and tests for reading more information from DNA[7] have increased the reliability of DNA evidence in the criminal process.[8] In the criminal context, it is therefore generally understood that DNA matching has a significant advantage over previous techniques such as fingerprints in terms of accuracy in identifying individuals.[9]

1.2 A Brief Overview of DNA Matching

DNA samples may be taken from an individual in many different ways, ranging from non-intrusive methods, either with the knowledge of the individual or surreptitiously (e.g. from a discarded Kleenex or cigarette)[10], to minimally intrusive methods (e.g. a cheek swab) to highly intrusive methods (e.g. a blood sample).[11] The other manner in which DNA samples may be obtained is from crime scene stains. At crime scenes, DNA may be found on a victim, a weapon or any other item at the scene, and may include blood, semen, hair or other sources of DNA samples.

The fact that the quality of the sample is better when it is from more intrusive sources,[12] raises questions of the most efficient, yet ethical, manner of collecting DNA

[6] *Id*.
[7] *See* infra at s. 4.3.1 for a discussion of the types of information currently derivable from a DNA sample.
[8] See e.g. Julie A. Singer, Monica K. Miller & Meera Adya, *The Impact of DNA and Other Technology on the Criminal Justice System: Improvements and Complications*, 17 Alb. L.J. Sci. & Tech. 87 (2007) [hereinafter "Singer"] at 96.
[9] *Id.*
[10] *See e.g. id.* at 97 and Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34 J.L. Med &Ethics 153 [hereinafter "Rothstein & Talbott"] at 156.
[11] *See e.g.* Nuffield Report, *supra* note 3 at s. 2.6.
[12] *Id*.

samples from individuals. In Canada, for example, 98.5% of the DNA samples taken for the national DNA databank from convicted offenders came from blood, while 1.4% came from mouth swabs and 0.1% from hair.[13] Since all samples in Canada are taken under a judicial warrant,[14] consent to the more intrusive methods is not required by law. While it is beyond the scope of this paper to examine issues of bodily privacy, it is important to understand that even before any personal information is derived from the DNA samples, the mere taking of the DNA sample can already raise privacy issues.

A brief overview of "DNA matching" is helpful at this stage as the term figures prominently throughout the paper below. Deoxyribonucleic acid (DNA) exists in every cell. It contains what has been described as the "'blueprint' for the physical make-up of each individual."[15] The DNA in every cell of one person is the same, but differs from every single other person (except an identical twin)[16] extremely slightly, but enough that techniques have been developed to create DNA profiles, a numeric representation of the DNA sample it relates to, in order to differentiate and identify individuals.

The common method for creating a DNA profile involves the analysis of a certain number of so-called "short-tandem-repeat" (STR) markers dispersed throughout the DNA.[17] An STR marker is a location of a short sequence of DNA in which a small set of base pairs (usually between 2-6) are repeated a different number of times in each individual.[18] These

[13] National DNA Data Bank Update, August 18, 2008, available at http://www.nddb-bndg.org/stats_e.htm (last updated 12 March, 2008) [hereinafter "DNA Data Bank Update"].
[14] For a full discussion of the collection process in Canada and the United Kingdom, see *infra* at Chapter 2. While similar statistics were not found for the United Kingdom, given that a non-intimate sample (mouth swab or hair) may be taken without consent, while intimate samples (blood) may only be taken with consent, even following conviction, it is probable that most samples are from non-intimate sources.
[15] Rebecca Sasser Peterson, *When Fear Goes Too Far,* 37 Am. Crim. L. Rev. 1219 at 1221 [hereinafter "Peterson"], citing J. Clay Smith, *The Precarious Implications of DNA Profiling*, 55 U. PITT. L. REV. 865, 869 (1994).
[16] Note, however, that recent research suggests that identical twins may not in fact have identical DNA, The Anahad O'Connor, New York Times, *The Claim: Identical Twins Have Identical DNA*, March 11, 2008, available at: http://www.nytimes.com/2008/03/11/health/11real.html?_r=1& ref=science&oref=slogin, cited in Frederico & Rondinelli's DNA Netletter, April 1, 2008 - Issue 99.
[17] See e.g. Nuffield Report, *supra* note 3 at s. 2.7;
[18] Forensic Data Center, *Short Tandem Repeats,* available at: http://www.forensicdnacenter.com/dna-str.html (last visited 10 October, 2008).

particular markers are called "non-coding" markers, as information beyond confirmation of an identity match cannot be derived from their analysis in this manner.[19] The number of STR markers analyzed in a DNA profile varies from country to country. The test used by Canada and the United States uses thirteen markers plus an indicator of gender,[20] while the United Kingdom uses ten markers plus an indicator of gender.[21] A DNA profile, therefore, consists of the "allele" numbers, being the number of times each marker is repeated. This means that in the UK, for example, where 10 markers are recorded, a DNA profile consists of a series of 20 numbers and an indicator of the sex of the individual.[22] Based on the North American test, with 13 markers, it is suggested that unrelated individuals will match on only 1 out of 13 of the STR locations, whereas related individuals will share more, with siblings matching in about four of these locations on average.[23] The odds that two individuals will match on all 13 of the STR locations is said to be one in a billion.[24]

Once a DNA profile is created, it is entered into databases in accordance with the applicable legal framework. The processes in Canada and the United Kingdom are described in more detail in Chapters 2 and 3, but generally, DNA profiles will be stored in one of two databases (or different portions of one database): (i) one containing identified DNA profiles; and (ii) one holding unidentified (e.g. crime scene) DNA profiles. DNA matching, therefore, is the process of comparing DNA profiles in order to observe the closeness of the match.

Once a DNA databank is in operation, there are several uses that can be made of it in respect of DNA matching. In the case of a new, unidentified, crime scene DNA sample, a

[19] See e.g. Pilar N. Ossorio, *About Face: Forensic Genetic Testing For Race And Visible Traits*, 34 J.L. Med. & Ethics 277 [hereinafter "Ossorio"] at fn 23. See however s. 4.3.1 infra for the types of information beginning to be inferable from a DNA profile.
[20] Carman Baggarley, Senior Policy Advisor, Office of the Privacy Commissioner of Canada, telephone call Sept. 3, 2008 [hereinafter "OPC Interview"]
[21] Nuffield Report, *supra* note 3, at s. 1.10.
[22] Nuffield Report, *supra* note 3 at s. 2.8.
[23] Rothstein & Talbott, *supra* note 10 at 156.
[24] U.S. Department of Energy, Office of Science, Human Genome Project Information, *DNA Forensics,* available at: http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml (last updated September 16, 2008).

DNA profile will be created and will be tested to see if it matches any DNA profile already identified in the database. If identified, the new DNA profile can also be run against the database of unidentified DNA profiles, to yield information as to the perpetrator of previously unsolved crimes. Even if the crime scene DNA profile was not identified, a test against other unidentified crime scene DNA profiles may nonetheless identify whether the same individual, although unknown, could be implicated in other unsolved crimes.[25]

1.3 DNA Evidence in Criminal Proceedings

The availability of DNA matching procedures has had enormous consequences on criminal prosecutions, to the delight of law enforcement agencies (and presumably to the dismay of offenders). The introduction and weight of DNA evidence in a criminal proceeding is subject to national criminal procedure law, a detailed discussion of which is beyond the scope of this paper. For the purposes of this paper, an overview of the general significance of DNA evidence will provide sufficient background to understand the implications of its use.

In the criminal context, in which proof "beyond a reasonable doubt" must be met, the accuracy and weight of evidence is key to prosecution.[26] Problems with relying on other types of evidence in criminal prosecution stem from the fact that "…eyewitnesses make errors, people falsely confess to crimes, and, most importantly, we may not always be able to look at circumstances after the fact and judge who are accurate eyewitnesses or who are coerced confessors."[27] For this reason, DNA evidence, with its high accuracy and scientific methodology, has been revolutionary in the courtroom.

Complicating reliance on this new form of evidence, however, is the fact that such evidence is more difficult to explain, in substance and evidentiary significance, to juries, than, for example, an eyewitness account would be. It has been found that juries "are likely

[25] For an overview of the types of matches sought, see e.g. National DNA Data Bank, available at: http://www.nddb-bndg.org/main_e.htm (last updated 1 September, 2006).
[26] *See e.g.* Singer, *supra* note 8 at 98.
[27] *Id.* at 100.

to commit serious mathematical errors when dealing with probabilistic evidence such as DNA match statistics"[28] and that certain ways of explaining probability to a jury will yield different results.[29] An example of increased willingness to rely on DNA evidence is seen in the United States, where it has been noted that a recent trend is:

> …a willingness to accept less certain information-and a higher frequency of false positives-in individual decisions, again often in the antiterrorism context […] [F]or some of the same reasons, data matching and mining results and other forms of less certain evidence are now used not only to trigger investigation, but also as the sole basis for judicial action.[30]

On the other side, there has also been observed the phenomenon of the so-called "CSI Effect,"[31] which suggests that as a result of watching too many crime shows on television, juries "have unrealistic expectations of what real life crime labs, police, and prosecuting attorneys are capable of doing. Prosecutors complain that these shows make it more difficult for them to secure convictions because jurors do not understand that scientific evidence is not available or even relevant in many cases."[32] This can hurt a prosecution's case in a way that using other types of evidence may not have.

Regardless of its use in a courtroom, the initial ability of DNA evidence to identify an individual is itself not infallible. The process of collecting and using DNA for evidentiary purposes is subject to attempts at circumvention by the individuals giving samples. Beginning with the example of the first DNA-based conviction, the Pitchfork case discussed above[33] in which a murderer had a friend give a DNA sample in his name, examples abound of creative ways in which individuals have tried to avoid being caught through a DNA match. In one case, a Canadian doctor accused of drugging and raping one of his patients provided a false blood sample by surgically inserting a plastic tube filled with another patient's blood into his

[28] Singer, *supra* note 8 at 108.
[29] *Id.,* citing Jason Schklar & Shari Seidman Diamond, *Juror Reactions to DNA Evidence: Errors and Expectancies*, 23 Law & Hum. Behav. 159, 160 (1999) at 162.
[30] Daniel J. Steinbock, *Data Matching, Data Mining, And Due Process*, 40 Ga. L. Rev. 1 at 6-7 (2005).
[31] See, e.g. Singer, *supra* note 8 at 113.
[32] *Id.* at 108, citing Richard Willing, "CSI Effect' has Juries Wanting More Evidence, USA Today, Aug. 5, 2004, available at: http://www.usatoday.com/news/nation/2004-08-05-csi-effect_x.htm?loc=interstitialskip.
[33] *Supra* at 2.

arm. That way, when the police took a sample, the blood drawn would not be his and the DNA would not match that from the sperm found with the crime scene victim.[34] The doctor was eventually convicted when a private investigator hired by his accuser took a sample of the doctor's DNA from a stolen chapstick and an envelope that he had licked, both of which matched the crime scene stain.[35]

As expressed above, DNA evidence, while an improvement over earlier technologies and methods of investigation and evidence gathering, is not perfect. Apart from scientific or technological limitations, it has been noted that while DNA "is generally accurate, human error can make it detrimental."[36] It is subject to circumvention, manipulation, error and misunderstanding (by both those giving and those analyzing the samples) and as such both prosecutors and policy-makers must consider the appropriate conditions in which DNA evidence should be used.

1.4 Nothing to Hide; Nothing to Fear?

A counter-argument often raised in response to concerns about the State handling citizens' personal information is that if someone has nothing to hide, then they should have nothing to fear from the state having access to their personal information.[37] The line of argumentation would suggest that that an innocent person has no reason to fear his or her genetic samples and related profile information being held in a State's forensic databank. The "nothing to hide, nothing to fear" argument is particularly relevant in the recent anti-terrorism, heightened-security, climate, when the weakening of privacy and data protection by the State is often framed as a necessary trade-off in the name of national security issues. Canada's Privacy Commissioner captured this in noting that Canada's "Anti-terrorism Act —

[34] Tania Simoncelli, *Dangerous excursions: the case against expanding forensic DNA databases to innocent persons*, Journal of Law, Medicine & Ethics. 34.2 (Summer 2006): 390(8) [hereinafter "Simoncelli"] at fn 33, citing http://www.hbo.com/autopsy/episode/episode_7_the_good_doctor.html [hereinafter "The Good Doctor"].
[35] The Good Doctor, *id.*
[36] Singer, *supra* note 8 at 112.
[37] Paul Chadwick, *The Value of Privacy,* E.H.R.L.R. 2006, 5, 495 [hereinafter "Chadwick"] at 504-5.

as well as other recent government initiatives aimed at combating terrorism — reflects a fundamental shift in the balance between national security, law enforcement and informational privacy, with a associated loss of privacy and due process protections for individuals."[38]

Against the "nothing to hide, nothing to fear" position, it has been argued that the utility of the argument is questionable as it places the onus on the wrong party[39] and "ignores any intrinsic value that might be placed on liberty, privacy and autonomy."[40] This counter-position contends that the starting point in a free society should be a "presumption of liberty,"[41] where citizens are under no obligation to justify why they do not want to give the government their personal information (let alone their *most* personal information – their genetic make-up); rather it is the government who must justify to the citizen why it is necessary to provide such information.[42] From this argument it follows that there must be sound justifications for collecting DNA samples for forensic purposes, and likewise for any other purpose for which that genetic information is intended to be used. For example, where DNA samples are actually helpful in an investigation and/or prosecution there may therefore be a greater justification for it's collection than where DNA samples are taken in respect of crimes for which DNA evidence is irrelevant to their investigation and prosecution.[43]

Even if one is comfortable with the "nothing to hide; nothing to fear" argument in the criminal context, the argument does not address the full extent of potential data protection issues. The argument's assumption is that if one is not a criminal, then their DNA will not be used against them in a criminal context.[44] Even if that is true, the fact that one's DNA is on

[38] Statement by Privacy Commissioner of Canada to the Subcommittee on Public Safety Act and National Security, June 1, 2005, available at: http://www.privcom.gc.ca/speech/2005/sp-d_050601_e.asp;
[39] Chadwick, *supra* note 37 at 505.
[40] Nuffield Report *supra* note 3 at s. 3.24.
[41] *Id*. at s. 3.26.
[42] See e.g. *Id.* and Chadwick, *supra* note 37 at 505.
[43] See *infra* at s. 4.1.
[44] See e.g. Chadwick, *supra,* note 37 and *Regina v. Chief Constable of South Yorkshire Police (Respondent) ex parte LS (by his mother and litigation friend JB) (FC) (Appellant) and Regina v. Chief Constable of South*

record with the State potentially exposes the individual to data protection issues that extend beyond the criminal realm, including the potential to reach other aspects of one's life such as health, insurance, employment and family. These risks are outlined below in this Chapter 1 and then discussed in more detail in Chapter 4.

1.5 Protection of Genetic Information (and Why it Matters)

In order to understand the potential data protection implications of a forensic DNA databank, it is important to underline the relationship between privacy and data protection, and specifically the significance of control over one's personal information. DNA collection by the State engages at least two aspects of privacy: (i) spatial privacy; and (ii) informational privacy.[45] There is said to be an infringement of one's spatial privacy when, for example, biological samples are taken without consent.[46] For this reason, interference with one's body is generally considered to require a higher standard of justification as well as the consent of the individual involved.[47] Informational privacy, on the other hand, which the remainder of this paper will focus on, relates to information about oneself, regarding which one would want to control the dissemination.[48] In this "informational privacy" therefore, lies the connection between privacy and data protection which this paper will focus on below.

Privacy law, at least in the Canadian context, has been described as being "generally about control over personal information, rather than privacy in broader terms of being left alone…"[49] The connection between privacy and data protection in the forensic DNA context was summarized by Arbour J., writing for the Supreme Court of Canada, as follows:

Yorkshire Police (Respondent) ex parte Marper (FC) (Appellant) (consolidated appeals) [2004] UKHL 39 [hereinafter "Marper – House of Lords"] at para. 37.

[45] See e.g. Nuffield Report, *supra* note 3, at ss. 3.7 and 3.8; and Emanuel Gross, *The Struggle Of A Democracy Against Terrorism--Protection Of Human Rights: The Right To Privacy Versus The National Interest--The Proper Balance*, 37 Cornell Int'l L.J. 27 [Hereinafter "Gross"] at 31

[46] Nuffield Report, *supra* note 3 at s. 3.7.

[47] *Id*.

[48] Nuffield Report, *supra* note 3 at s. 3.8.

[49] A. Wayne McKay, "Human Rights in the Global Village: The Challenges of Privacy and National Security", 20 Nat'l J. Const. L. 1 (2006) [hereinafter "McKay"] at 7.

> The informational aspect of privacy is also clearly engaged by the taking of bodily samples for the purposes of executing a DNA warrant. In fact, this is the central concern involved in the collection of DNA information by the state. Privacy in relation to information derives from the assumption that all information about a person is in a fundamental way his or her own, to be communicated or retained by the individual in question as he or she sees fit (per La Forest J. in Dyment, [[1988] 2 S.C.R. 417] at p. 429). There is undoubtedly the highest level of personal and private information contained in an individual's DNA.[50]

In this view of privacy rights, "privacy can also be violated by allowing access to personal information for a purpose beyond those that were originally intended."[51] This is precisely one of the risks that presents itself with respect to genetic materials and information held in a forensic DNA databank. For that reason, the legal framework in which the DNA databank operates must be examined for how it limits opportunities for such secondary purposes to be realized.

1.6 Data Protection Issues in the Forensic DNA Databank Process

Scientific and technological improvements in techniques related to DNA profiling may increase convictions and improve accuracy (i.e. securing convictions of the guilty and not convicting the innocent) over convictions made in reliance on DNA evidence created previously with less sophisticated technology. Despite these positive advances, however, concerns related to the handling of DNA by the state remain, including the protection afforded by law to the genetic information held in a forensic DNA databank.

Stemming from DNA's advantages over earlier techniques such as fingerprints are issues that were not present to the same degree with respect to fingerprint databases. While fingerprints can only reveal the identity of an individual, but no further information, with DNA there is the "possibility of deriving additional information about an individual by further analysis of their DNA, and about family relationships by comparing profiles."[52] Of

[50] *R v. S.A.B*. [2003] 2 S.C.R. 678 (Supreme Court of Canada) [hereinafter "*R. v. S.A.B*." at para. 48.
[51] McKay, *supra* note 49. See also Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. Ottawa L. & Tech. J. 357 (2005) [hereinafter "Levin"] at 392-393.
[52] Nuffield Report, *supra* note 3, at s. 1.19.

concern is that at each stage in the process of collecting, storing, using and sharing DNA samples in a forensic DNA databank there is potential for the DNA to be used, alone or in connection with information stored in other databases, for secondary purposes, without the consent of the individuals involved. For example, as suggested by Chief Justice Moyer of the Supreme Court of Ohio, there is concern about "the propriety of using genetic information to discriminate against individuals for insurance or employment purposes."[53] These are but a few of the potential uses for information derivable from a DNA sample.

These secondary uses could come about clandestinely, for example through unauthorized analysis on a DNA sample beyond that required for the forensic analysis or through cross-referencing the genetic information drawn from the individual's DNA with information about the individual housed within other governmental or private sector databanks. Alternatively, such secondary uses, employing the same methods of testing and cross-referencing, can lawfully result from what has been referred to as "function creep", the expansion of permitted uses of information collected for a specific purpose.[54] Concerns related to function creep acknowledge the risk that "informal laws may one day be changed to allow outside companies, such as health insurance providers, access to the information."[55]

The above demonstrates the potential, whether in the present or in the future, to use forensic DNA samples to derive extremely sensitive, information about an individual. Chapter 3 of this paper will examine the measures put in place to regulate the uses made of DNA samples, and their derivative DNA profiles, collected in Canada and the United Kingdom and Chapter 4 will discuss the present and potential information derivable from such a sample. Limitations on who is included in the DNA databank to begin with and legal requirements regulating the length and conditions for the retention of DNA samples will also

[53] Moyer, *supra* note 2, at 687.
[54] See, e.g. Singer, *supra* note 8 at 123.
[55] *Id.*, citing Paul E. Tracy & Vincent Morgan, *Big Brother and His Science Kit: DNA Databases for 21st Century Crime Control?* 90 J. Crim. L. & Criminology 635, 688-89 (2000) [hereinafter "Tracy"].

have an obvious effect on the scope of who will be affected by any of the issues discussed above. In what follows, this paper will argue that given the importance of individuals maintaining control over their personal information, as discussed above, the treatment of DNA in government care should be appropriately designed to account for its particular sensitivity.

CHAPTER 2 –

FORENSIC DNA DATABASE REGIMES IN CANADA AND THE UNITED KINGDOM

At each stage of collection, retention, use or sharing of forensic DNA data there exist risks to the protection of the personal information that it contains. The legal frameworks regulating forensic DNA databanks and handling of genetic information are therefore the first place to look for how these issues are dealt with in a particular national regime. In this Chapter and Chapter 3, the forensic DNA databank regimes in Canada and the United Kingdom will be discussed. First, a general overview of the legislative frameworks creating and regulating the operation of the national DNA databanks in Canada and the United Kingdom will be reviewed. Then, the two systems will be described and compared with respect to: (i) conditions for inclusion in the national forensic DNA databank; (ii) destruction and retention requirements; (iii) restrictions on secondary uses; and (iv) restrictions on sharing of information stored in the forensic DNA databank. The differences in approaches in respect of each of the above are reflective of national legal and policy decisions surrounding the administration of each national DNA databank.

2.1 Legislative Frameworks

2.1.1 Canada

In Canada, there are two parallel legislative regimes regulating Canada's "National DNA Data Bank". One legislative regime applies to the collection of DNA through the issuance of warrants in the process of a criminal investigation[56] and the other regulates the collection of DNA from convicted offenders and the maintenance of the National DNA Data Bank.[57] Regardless of whether DNA is being collected in the course of an investigation or

[56] *Criminal Code* R.S., 1985, c. C-46.
[57] *DNA Identification Act*, 1998, c. 37 at ss. 5(3) and 5(4). See also description of parallel systems in R. *v. S.A.B.*, *supra* note 50 at para. 3.

from a convicted offender, Canada's *Criminal Code* sets out the conditions under which a court can issue a warrant or make an order for the collection of a DNA sample for inclusion in the Data Bank, including the list of offences in respect of which a DNA sample may be taken (discussed below).

Canada's *Privacy Act*[58] regulates the handling of personal information by the government in general terms, but its provisions regarding use and disclosure are subject to other, more specific, acts of Parliament.[59] Once a DNA sample has been collected in accordance with the *Criminal Code*, the *DNA Identification Act* regulates the collection, use, retention and disclosure of that DNA sample, any DNA profile created or other personal information collected or derived. The Canadian system maintains two indexes as part of its National DNA Data Bank system: (i) a crime scene index, containing unidentified DNA profiles collected from crime scenes; and (ii) a convicted offender index, containing DNA profiles collected from convicted individuals in accordance with the *Criminal Code*.[60] The head of Canada's national police force, the Royal Canadian Mounted Police, (the "RCMP Commissioner") has the statutory duty of maintaining the DNA Data Bank.[61]

2.1.2 The United Kingdom

The United Kingdom maintains one "National DNA Database," which contains DNA profiles from DNA samples taken from those arrested for certain offences (discussed below) as well as crime scene samples and "elimination" samples from volunteers and victims.[62] The regulatory framework in the United Kingdom differs in structure from that in Canada. Critics of the regulatory regime in the United Kingdom have noted that "[t]he current regulatory structure for bioinformation databases is not on a statutory footing and the legislative

[58] R.S., 1985, c. P-21.
[59] *Id*. at s. 8 (2).
[60] *DNA Identification Act, supra* note 57 at s. 3 and s. 4.
[61] *Id.* at s. 5(1).
[62] See e.g. Nuffield Report, *supra* note 3 at s. 1.21

framework surrounding the forensic use of bioinformation is piecemeal and patchy."[63] This criticism appears, in fact, quite accurate.

Originally the powers to take samples came from the *Police and Criminal Evidence Act, 1984*[64] ("PACE"), which was then amended by the *Criminal Justice and Public Order Act, 1994*[65] to permit police to take and retain certain DNA samples without consent. This permitted (but did not specifically regulate) the creation and operation of the United Kingdom's National DNA Database.[66] Building on top of the powers granted by earlier legislation, additional significant pieces of legislation were passed, including the *Criminal Justice and Police Act, 2001*,[67] which covers the retention and searching of DNA samples and profiles[68] and the *Criminal Justice Act, 2003*,[69] which broadened the scope of which stage in the criminal process DNA could be taken and retained.[70] The implications of these piecemeal changes will be discussed in further detail below. From this introduction to the two regulatory regimes, it already appears that the Canadian framework is more grounded in legislation, making information about the DNA databank regime more accessible and understandable to the public, to whom it applies.

[63] *Id.* at Executive Summary, para. 48.
[64] (1984, c. 60) [hereinafter "PACE"].
[65] (1994, c. 33).
[66] Genewatch UK, *A Brief Legal History of the NDNAD*, available at http://www.genewatch.org/sub-537968.
[67] (2001, c. 16).
[68] *Id.* at s. 4.12.
[69] (2003, c. 44).
[70] *Supra* note 63.

2.2 Conditions For Inclusion In National Forensic DNA Databanks

A preliminary factor relevant to the creation of a forensic DNA databank, is the threshold which must be met in order for an individual to be included in that databank. Where this threshold is set at in the applicable laws is reflective of national criminal policy and, as will be discussed below, is approached differently in Canada and the United Kingdom. The United Kingdom has a significantly lower threshold for inclusion in the national DNA databank than exists in Canada. One result of this low threshold[71] is that the United Kingdom's National DNA Database includes a much higher percentage of its population than any other country in the world, approximately six percent.[72] As an illustration of the difference, the next highest percentage of population included in a national forensic DNA databank is found in Austria, with a significantly lower rate of 1.04% of the population included.[73] The United States' forensic DNA databank is larger in terms of total numbers of samples,[74] but only covers approximately 0.5% of the population.[75] By further contrast, Canada's National DNA Data Bank, holds 183,949 DNA profiles,[76] totaling approximately 0.005% of Canada's population.[77]

If more are people included in a national NDA databank, more people will be affected by any uses of information in that databank and will suffer the consequences of any unauthorized use or other data protection breach. For this reason, the thresholds applicable to who is included in the DNA databank are important to examine, along with the justifications

[71] Home Office Forensic Science and Pathology Unit, "DNA Expansion Programme 2000–2005: Reporting Achievement", available at: http://police.homeoffice.gov.uk/publications/operational-policing/DNAExpansion.pdf [hereinafter "Reporting Achievement"].
[72] Nuffield Report, *supra* note 3 at s. 1.22. Note that United Kingdom also holds over 6.5 million fingerprints in a parallel regime for fingerprinting. This database includes approximately 20 percent of the United Kingdom's male population and five percent of the female population, *id.* at s. 1.17.
[73] Hansards, available at: http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo060418/text/60418w75.htm - 60418w75.html_spnew5statistics are from 2005. (hansard); see also Genewatch, Facts and Figures, available at: http://www.genewatch.org/sub-539481.
[74] Nuffield Report, *supra* note 3 at s. 1.2.
[75] *Id.* at s. 1.22.
[76] DNA Data Bank Update, *supra* note 13.
[77] 183,949 divided by Canada's official population as of July 1, 2008 available at Statistics Canada, http://www.statcan.ca/Daily/English/080929/d080929b.htm (last updated September 29, 2008).

for where the lines are drawn. Below, this section will examine the thresholds for collection of individuals' DNA samples in the forensic context, and the inclusion of the individuals in the both national forensic DNA databank regimes examined in this paper. The criteria for inclusion in Canada and the United Kingdom will be compared below with respect to: (i) the type of offences for which the taking of DNA samples is authorized; (ii) the timing of taking the DNA sample (i.e. whether upon arrest vs. only upon conviction); and (iii) what form, if any, of judicial intervention is required before a sample is taken.

2.3 Offences For Which DNA Can Be Collected

2.3.1 Canada

In Canada, the forensic DNA databank regime applies to those investigated or convicted in respect of offences which are defined in Canada's Criminal Code as either "primary designated offences" or "secondary designated offences." Primary designated offences are defined by an exhaustive list of criminal offences, generally of a more violent nature, including murder, sexual assault, hostage taking and kidnapping.[78] Secondary designated offences similarly are defined by an exhaustive list, this one containing criminal offences of a less extreme nature than primary designated offences, but still of a certain degree of harm or apparent future risk. Secondary designated offences include any offence under the Criminal Code carrying the possibility of five years or more of incarceration (other than primary designated offences) and a list of specific offences including, *inter alia*, robbery, assault, dangerous operation of a vehicle causing bodily harm or death and failure to stop at the scene of an accident.[79]

It is noteworthy that the list of primary designated offences was expanded in 2001 by the addition of new offences created by Bill C-36, Canada's *Anti-Terrorism Act.*[80] The

[78] Criminal Code, *supra* note 56 at s. 487.04
[79] *Id.*
[80] 2001, c. 41.

category of primary offences now also lists terrorism-related offences, including, *inter alia*, participating in, or committing an offence for a terrorist group and facilitating terrorist activity.[81] Concerns expressed by Canada's Privacy Commissioner, Jennifer Stoddart, amongst others, with respect to the continuing expansion of the list of primary and secondary designated offences, and consequentially the expansion of the DNA databank itself, will be addressed in Chapter 4, below.

2.3.2 United Kingdom

The *Criminal Justice Act, 2003* amended the *Police and Criminal Evidence Act, 1984* to provide that a DNA sample may be taken from a person detained following his or her arrest for a "recordable offence".[82] A recordable offence includes any offence that carries the possibility of incarceration, as well as a number of other offences that do not carry the possibility of incarceration, but are classified as "recordable offences" by applicable regulations.[83] This list of additional, less serious, offences has expanded over time through amendments to a schedule to the *National Police Records (Recordable Offences) Regulations.*[84] At the time of writing, recordable offences include a long list of offences of a more minor nature, ranging from failing to give notice of a public procession[85] to "trying to enter designated sports ground while drunk"[86], entering land for the purpose of destroying rabbits[87] to "taking or riding a pedal cycle without owner's consent."[88]

From the fact that a DNA sample may be taken in respect of this list of relatively minor offences, the difference in approach between Canada and the United Kingdom with

[81] *Supra* note 56 at s. 487.04.
[82] *Supra* note 69 at s. 10(2).
[83] Nuffield Report, *supra* note 3 at Box 1.2; National Police Records (Recordable Offences) Regulations 2000, S.I. 2000/1139 at s. 3(1), as amended. [hereinafter "Recordable Offences Regulations"].
[84] Schedule to the Recordable Offences Regulations 2000, *id.*, as amended by S.I. 2003/2823 and S.I. 2005/3106 [hereinafter "Recordable Offences Schedule"]. This schedule contains a list of recordable offences.
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] S.I. 2000/1139.

respect to inclusion in the national forensic DNA databank is emerging. The greater breadth of offences resulting in inclusion in the forensic DNA databank in the United Kingdom is indicative of a policy favouring inclusion of the population in the United Kingdom's databank, which can be contrasted with Canada's approach of limiting the numbers included.

It is noteworthy that voluntary samples, for example those given by eyewitnesses in order to exclude themselves from suspicion, are included in the United Kingdom's National DNA Database only with the consent of the individual. Once included, however, they are held in the same database and without any differentiation of status indicated in the NDNAD or in its treatment.[89] This means that in the case of any other use or sharing made of the DNA samples or profiles, volunteers are treated the same as those suspected or convicted of criminal activity. While volunteer samples are only added to the National DNA Database with consent, that consent is irrevocable.[90] This is based on the theory that individuals would otherwise simply have themselves removed from the databank before committing a crime, as well as the government's desire to avoid situations where samples which should have been removed when consent was revoked, were not removed, and then issues related to admissibility of evidence may arise. [91] Both the Nuffield Council and the House of Commons Science and Technology Committee conclude that, consistent with the principles of consent in the medical context, volunteers should be permitted to revoke their consent to having their DNA profile stored in the databank.[92]

By contrast, in Canada, volunteer samples are never included in the National DNA Data Bank.[93] While such samples may be taken during the course of an investigation, they

[89] Nuffield Report, *supra* note 3 at s. 1.2.1.
[90] *Id.* at s. 4.58.
[91] *Id.* at s. 4.60.
[92] *Id.* at Executive Summary, s. 15; and House of Commons Science and Technology Committee, *Forensic Science on Trial*, Seventh Report of Session 2004-2005, available at: http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/9607.htm [hereinafter "Forensic Science on Trial"] at para. 75.
[93] OPC Interview, *supra* note 20.

could be neither added to nor retained in the National DNA Data Bank as there is no provision for this in Canadian law, which permits inclusion in the National DNA Data Bank only following a judicial decision as discussed above.[94] The inclusion of volunteer samples is one of several issues that was to be reviewed in the statutorily mandated five-year-review of the *DNA Identification Act,*[95] but the review is already several years overdue and had not been scheduled as of the date of this paper.[96]

With respect to voluntary samples, critics have noted that what appears to be consent, may be something less than voluntary. In a 2003 high profile murder investigation of a young girl in Toronto, Canada the police asked men in the neighbourhood to provide a DNA sample on the understanding that the samples would be destroyed after the investigation for those cleared from suspicion. A prominent Canadian criminal lawyer noted at the time that "[t]here's enormous pressure to assent to the police request…To call it consent is a little disingenuous."[97] Likewise, Alan Borovoy of the Canadian Civil Liberties Association noted that "[a]nybody who says no is likely to anticipate very unpleasant consequences of saying no. So there is a heavy coercion to it."[98] In that case, only two of the 300 men requested to volunteer a DNA sample refused. One of those two men was ultimately convicted for her murder following a match from his DNA taken from a discarded pop can against a crime scene sample.[99]

[94] *Id.*
[95] DNA Identification Act, *supra* note 56 at s. 13.
[96] OPC Interview, *supra* note 20.
[97] CBCNews.ca, "DNA Samples Invade Privacy, Critics Say", May 23, 2003, available at: http://www.cbc.ca/canada/story/2003/05/23/jone030523.html.
[98] CTV.ca "TO Police Defend Requesting DNA Samples", May 22, 2003, available at: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20030522/hollyjones_investigation_20030522?s_name=Autos&no_ads=.
[99] Rick Westhead, "Widen DNA Dragnet: Blair", April 12, 2008, available at: http://www.thestar.com/News/GTA/article/413851.

2.4 Timing of Taking the DNA Sample and Whether Judicial Intervention Required

Additional factors relevant to who is ultimately included in a DNA databank are the timing of the sample being taken and the standard of judicial review required before a DNA sample may be taken and included in the DNA databank. Due to the natural attrition during the criminal process,[100] taking samples upon arrest will result in collecting DNA samples from more people than if samples were collected only upon conviction.

At whichever stage of the criminal process DNA samples are taken, it is equally relevant whether there is any discretion, judicial or otherwise, before samples are taken for inclusion in the databank. Arguably, lacking a process whereby a reviewing body has discretion to refuse to permit the taking of samples will contribute to the creation of a larger forensic DNA database.

2.4.1 Canada

In Canada, DNA samples may only be taken upon the issuance of a judicial warrant,[101] whether at the investigative stage or following conviction. During the investigative stage, an application is made to a provincial court judge, who must first evaluate whether there are reasonable grounds to believe:

> (a) that a designated offence has been committed,
>
> (b) that a bodily substance has been found or obtained [at the crime scene]
>
> (c) that a person was a party to the offence, and
>
> (d) that forensic DNA analysis of a bodily substance from the person will provide evidence about whether the bodily substance referred to in paragraph (b) was from that person. [102]

If the above criteria are met and the judge is satisfied that "it is in the best interests of the administration of justice to do so", he or she may issue a warrant authorizing taking "any number of samples of one or more bodily substances that is reasonably required" for "the

[100] Nuffield Report, *supra* note 3 at s. 4.29.
[101] An exception to this is in the case of samples given voluntarily for the purpose of an individual eliminating him or herself as a suspect in the investigation, OPC Interview, *supra* note 20. As noted above, however, these volunteer samples may not be included in the National DNA Data Bank, see *supra* at s. 2.3.
[102] Criminal Code, *supra* note 56 at s. 487.05(1).

purpose of forensic DNA analysis."[103] The criteria requiring that taking a DNA sample is "in the best interests of the administration of justice" acts as a limit on including individuals in the DNA databank system in respect of whom the administration of justice would not require that. In determining whether to issue the warrant, the Criminal Code also states that the judge must "have regard to all relevant matters" including the nature of the offence and whether there is a appropriate person available to take the samples in accordance with the legal prescriptions for that process.[104]

A separate set of conditions apply for judicial orders for taking DNA samples upon conviction, varying depending on whether the offence in question is designated as a primary or secondary offence. Upon conviction[105] for a primary designated offence, a judge *must* make an order authorizing the taking of a sample for forensic DNA analysis,[106] unless the court:

> is satisfied that the person or young person has established that, were the order made, the impact on the person's or young person's privacy and security of the person would be grossly disproportionate to the public interest in the protection of society and the proper administration of justice, to be achieved through the early detection, arrest and conviction of offenders.[107]

By contrast, in respect of secondary designated offences, rather than the order being mandatory, the judge has the discretion to issue the warrant "if the court is satisfied that it is in the best interests of the administration of justice to do so.[108]" In making this determination, the Canadian Criminal Code requires that the court consider "the impact such an order would have on the person's or young person's privacy and security of the person."[109] Courts have refused to authorize the taking of samples from, for example, individuals with no previous criminal record of offences for which DNA would assist an

[103] *Id.*
[104] *Id.* at 487.05(2).
[105] *Id.* at 487.051(1). Note that the order must also be made in certain other specified cases, including, *inter alia*, a discharge or a conviction under the *Youth Criminal Justice Act* (2002, c.1).
[106] *Criminal Code*, *supra* note 56 at s. 487.051(1)(a).
[107] *Id.* at s. 487.051(2).
[108] *Id.* at s. 487.051(1)(b).
[109] *Id.* at s. 487.051(3).

investigation, or convicted of non-violent offence such as drug production or trafficking. An example of this is a recent Canadian decision from the province of Ontario, *R. v. Harris*[110] in which the Court refused to issue an order in respect of a man pleading guilty to cocaine trafficking. The Court held that, since the offender did not have "recent convictions for offences for which DNA identification would be a useful investigatory tool, I have difficulty in seeing the appropriateness of such an order in the case of a conviction for trafficking a small amount of a controlled substance."[111]

The above demonstrates the degree of judicial oversight and discretion involved before a DNA sample may be taken or an individual may be added to Canada's National DNA Data Bank, as well as the statutory requirement to consider the privacy implications of including them in the National DNA Data Bank. The result of this additional step of judicial intervention adds another stage at which individuals can be excused from inclusion in the National DNA Data Bank, which contributes to limit the number of individuals included.

2.4.2 United Kingdom

In the United Kingdom, as briefly mentioned above in respect of the range of "recordable offences", samples may be taken upon arrest for a recordable offence[112] without consent and without consideration of whether or not such biological evidence is relevant to investigative purposes.[113] The legislative patchwork governing the taking and retention of DNA samples has grown incrementally through successive legislation, as was noted above. The *Criminal Justice and Police Order Act, 1994* had permitted the taking of "non-intimate samples" (e.g. a mouth swab, or hair sample) from individuals charged with recordable offences.[114] The latest expansion, the *Criminal Justice Act, 2003*'s amendments to the *Police*

[110] [2008] O.J. No. 1976, Ontario Superior Court of Justice, D.M. Brown J., May 16, 2008.
[111] *Id.* at s. 47, cited in Frederico & Rondinelli's DNA Netletter, June 1 , 2008, issue 101.
[112] *PACE, supra* note 64 at para. 63(2).
[113] See e.g. commentary at Nuffield Report, *supra* note 3 at s. 1.23.
[114] Forensic Science on Trial, *supra* note 92 at para. 64.

and Criminal Evidence Act, 1984, now permits the taking of samples upon arrest, broadening the number of individuals who have samples taken.[115]

The permitted collection of a DNA sample upon arrest and detention without judicial intervention in the United Kingdom is in sharp contrast to the Canadian approach, which requires judicial approval and, in that process, consideration of, amongst other factors, the relevance that the DNA sample would have on the investigation and in certain cases, privacy implications.[116] The United Kingdom's approach to collection of samples, therefore, is consistent with the general approach of the forensic DNA databank regime in the United Kingdom which leans towards inclusion as the norm, rather than as an exceptional measure, which the Canadian system exemplifies. This will be examined further below in the context of retention of such personal information.

2.5 Safeguards Against Use Of DNA Profiles And Samples For Secondary Purposes

Once individuals are included in a national DNA databank, the next stages requiring regulation to protect the data relate to how the samples, profiles and associated personal information are stored, used and shared. It has been argued that "[w]hile the initial taking of such bioinformation raises some ethical issues, it is the retention of this bioinformation in searchable databases that is of more serious ethical concern."[117] This is because, by its nature, retained data presents future data protection risks that destroyed data does not. Factors affecting the degree of potential risk include which exact information is retained, how long it is retained for, and what conditions apply with respect to access to and sharing of that data.

2.5.1 The Type and Amount of Information Stored

In assessing potential data protection risks related to the storage of bioinformation for forensic purposes, the first significant distinction is whether the actual DNA samples

[115] *Id.* at para. 66. See *PACE*, *supra* note 64 at s. 63(2).
[116] See *supra* at s. 2.4.1.
[117] Nuffield Report, *supra* note 3 at s. 1.13.

themselves are retained, or only the DNA profiles created therefrom. The decision as to what other personal information related to the individual to whom the DNA relates is stored and how it is separated from and associated with the DNA sample or profile is also be discussed below.

2.5.2 Canada

Canada's *DNA Identification Act* specifies that both the crime scene index and the convicted offenders index will hold "DNA profiles."[118] A DNA profile is defined for the purposes of the Act as the "the results of forensic DNA analysis of a bodily substance," in other words, the result of the analysis of the DNA sample.[119] Additionally, in respect of each DNA profile, the National DNA Data Bank contains information required to establish:

> (a) in the case of a profile in the crime scene index, the case number of the investigation associated with the bodily substance from which the profile was derived; and
>
> (b) in the case of a profile in the convicted offenders index, the identity of the person from whose bodily substance the profile was derived.[120]

Measures are in place to protect the identity of the person to whom a DNA profile in the Convicted Offenders Index relates as well as the stored DNA sample.[121] When the DNA sample is first taken, the individual's personal information and fingerprints are entered onto one card. The DNA sample (blood, hair or buccal swab) is put on another card, with another set of fingerprints. This card with the DNA sample contains no personal information and is linked to the fingerprint card containing personal information by a bar code. Upon receipt by the Data Bank, the fingerprints are confirmed to ensure that the correct information is being linked to the DNA sample and the bar code number is entered into the databank. The sample is then sent for analysis and then DNA profile is entered into the Data Bank. The card containing fingerprints and personal information is then sent to a different part of the RCMP

[118] DNA Identification Act, *supra* note 56 at ss. 3 and 4.
[119] *Id.* at s. 2.
[120] Id. at s. 5(5)(a),(b).
[121] The following process is set out at the following website: National DNA Data Bank, *Protecting Privacy*, available at: http://www.nddb-bndg.org/pri_secu_e.htm.

building and to a different RCMP agency, the Information and Identification Services, and logged into their system.[122] In this manner, the DNA sample is separated, both physically and operationally, from the identifiable personal information about the individual. The National DNA Data Bank confirmed in an interview that those working with the DNA samples do not have access to personal information related to that individual, including his or her name.[123] Even those with access to only DNA profiles do not have the names related to the DNA profiles - when a match is found, the person matching DNA profiles calls the fingerprint bureau with the file number, who then can look at the offender's record based on the file number and find the necessarily related personal information.[124]

The Supreme Court of Canada has recognized that the forensic DNA regime minimizes violations of informational privacy by only conducting a DNA analysis on the non-coding DNA.[125] The Court specified that "[T]he DNA analysis is conducted solely for forensic purposes and does not reveal any medical, physical or mental characteristics; its only use is the provision of identifying information that can be compared to an existing sample."[126] The effects of technological, legal or regime changes on the above statement are considered in Chapter 4.

2.5.3 United Kingdom

A DNA profile on the National DNA Database in the United Kingdom contains the following information: (i) a number that is linked to a criminal record on a police database; (ii) information about the police force that collected the sample of DNA; (iii) the person's name, date of birth, ethnic appearance (as defined by the police) and gender; (iv) details of the type of biological sample from which the DNA is taken (blood, semen, saliva, etc.); (v)

[122] *Id.*
[123] Telephone call with Andre Savoie, acting manager, collection and training, National DNA Data Bank on 12 September, 2008 [hereinafter "NDDB Interview"].
[124] *Id.*
[125] *R. v. S.A.B., supra* note 50 at s. 49.
[126] *Id.*

the type of DNA test used; (vi) the DNA profile (a string of 20, two-digit numbers and a sex indicator); and (vii) a unique bar-code reference number (linking to the location of the stored DNA sample).[127] Similar to Canada, in the United Kingdom, DNA profiles are kept on the NDNAD, while DNA samples themselves are kept in storage separately, the difference appears to be, however, that more information is associated with the profile than in the Canadian system.

2.6 Destruction and Retention of DNA Samples and DNA Profiles

Sir Alec Jeffreys, the father of DNA fingerprinting, explained the difference between retaining DNA profiles and samples as follows: "If you have a DNA profile it is just a bunch of numbers on the computer and it really does not matter, but if you have the original DNA sample then you have the potential to extract absolutely every scrap of genetic information of that individual".[128] In favour of destroying DNA samples and retaining only the DNA profile in a databank, it has been argued that the retention of the DNA sample itself leaves open the risk related to future uses of the DNA sample for extracting further information, including through processes that may not even exist at the present time.[129] The potential for future uses of stored DNA samples to extract and use information secondary to the forensic purposes therefore arguably requires greater justification for the retention of DNA samples than for DNA profiles which have little use beyond forensic identification. It is noteworthy, however, that with advances in technology, DNA samples may also be used following conviction for forensic purposes true to their original purpose for collection, such as when new techniques permit re-testing of DNA samples to exonerate the wrongfully convicted.

[127] Nuffield Report, *supra* note 3 at box 1.3.
[128] Forensic Evidence on Trial, *supra* note 92 at 70.
[129] See e.g. Nuffield Report, *supra* note 3 at s 1.12; Michael E. Smith, "Let's make the DNA identification database as inclusive as possible.(DNA Fingerprinting and Civil Liberties)"Journal of Law, Medicine & Ethics. 34.2 (Summer 2006): 385(5). 2008 [hereinafter "Smith"].

In Canada, the *DNA Identification Act* and the *Criminal Code* govern the retention and destruction requirements applicable to DNA profiles and DNA samples in the National DNA Data Bank. With respect to DNA samples, the *DNA Identification Act* prescribes the mandatory destruction of DNA samples: (i) if a final judgment sets aside the order for the DNA collection; (ii) if a final judgment acquits the person of all designated offences to which the DNA order related; or (iii) one year after an absolute discharge or three years after a conditional discharge related to all designated offences.[130] This means that only convicted individuals' samples are retained in the National DNA Data Bank. The same Act also leaves discretion for the RCMP Commissioner to destroy retained DNA samples if he "considers that they are no longer required for the purpose of forensic DNA analysis."[131] This demonstrates an approach favouring exclusion from the National DNA Data Bank unless there is a justification for their retention.

The retention of DNA samples for the purpose of future analysis following technological advances is explicitly accounted for in the Canadian regime. A new forensic DNA analysis may be carried out on a stored DNA sample if "the Commissioner is of the opinion that the analysis is justified because significant technological advances have been made since the time when a DNA profile of the person who provided the bodily substances, or from whom they were taken, was last derived."[132] This approach highlights an important counter-argument to concerns regarding the retention of samples – while retention of the DNA sample may increase risk of harm with respect to future uses, being able to conduct new, state-of-the-art tests on retained older DNA samples also can be a very important manner of securing future convictions and/or exonerations.[133] On the other hand, such a provision could present a risk to the extent that it could be used in conjunction with

[130] DNA Identification Act, *supra* note 56 at ss. 10(7)(a), (b) and (c).
[131] *Id.* at 10(6).
[132] *Id.* at s. 10(2).
[133] See e.g. Nuffield Report, *supra* note 3 at s. 4.39.

technological advances as a justification for further extraction of information from a DNA sample, once that is possible. This risk is, however, mitigated by the rest of the legal framework limiting the use to creating the non-coding DNA profile and limiting the purposes for which both the DNA sample and profile may be used.

With respect to DNA profiles, the *DNA Identification Act* requires their indefinite retention, unless either the individual has been acquitted of the offence, or the conviction quashed.[134] The effect of this is that, like DNA samples, DNA profiles are only retained for convicted offenders.

2.6.1 United Kingdom

In sharp contrast to the practice in Canada, DNA profiles in the United Kingdom are retained indefinitely for each person arrested, whether or not they are ultimately convicted.[135] Originally, DNA profiles of those not convicted were to be deleted. Then it was found that over 50,000 DNA samples and DNA profiles were held in violation of the law, which proved an embarrassment for the Home Office when, upon finding a match, the offenders successfully argued that the DNA evidence had been illegally retained and they were being acquitted on that basis.[136] In 2001, the law was changed to permit the retention of DNA samples and DNA profiles of those *charged* with an offence, whether or not convicted.[137] Finally in 2003, the present law was put in place, which, as discussed above, permits the retention of DNA samples and DNA profiles of all those *arrested*, regardless of whether charges are ever laid.[138] Regarding cases in which a DNA profile would be removed from the DNA Database, a statement from the Association of Chiefs of Police Offices said that "[e]xceptional cases will, by definition, be rare. They might include cases where the original

[134] *DNA Identification Act*, *supra* note 57 at ss. 9(1) and 9(2).
[135] *Criminal Justice and Police Act, 2001*, *supra* note 67 at s. 82;
[136] *See e.g.* Forensic Science on Trial, *supra* note 92 at paras. 65-66; and Nuffield Report, *supra* note 3 at s. 4.37.
[137] *Criminal Justice and Police Act, 2001, supra* note 67 at s. 82(4).
[138] *Criminal Justice Act, 2003*, *supra* note 69 at s. 10.2.

arrest or sampling was found to be unlawful. Additionally, where it is established beyond doubt that no offence existed, that might, having regard to all the circumstances, be viewed as an exceptional circumstance."[139] A 2007 proposal by the Home Office would permit the retention with respect to all individuals charged with any offence, eliminating the use of the category of "recordable" offences.[140]

The Human Genetics Commission, a watchdog group funded to carry out a government inquiry as to public opinion on the National DNA Database, recommended that the profiles stored on the National DNA Database of one million innocent people should be destroyed.[141] Most members of the group were opposed to setting up a universal database, noting that "[b]y putting everyone on the database you are naming them as a possible suspect."[142]

Another example of the more inclusive approach in the United Kingdom is seen in the treatment of youths and children in the forensic DNA databank regimes. In Canada, only children above the age of 12 may be in the National DNA Data Bank and in a telephone interview with a representative of Canada's Privacy Commissioner's Office, it was confirmed that no data is held in the National DNA Data Bank on children under 12 years of age.[143] Further, DNA samples and DNA profiles of children between the ages of 12 and 17 who are in the National DNA Data Bank are subject to shorter retention periods than those of adults.

[139] Genewatch, "Exceptional Case Procedures for Removal DNA, Fingerprints and PNC Records", April 24, 2006, available at http://www.genewatch.org/sub-539488; see also: Where Is My Data?, "ACPO Guidelines for DNA Retention", 16 August, 2008, available at: http://www.whereisyourdata.co.uk/whereismydata/2008/08/16/acpo-guidelines-for-dna-retention/. For an article on how to get a DNA profile deleted from the National NDA Database, see David Mery, "How to Delete Your DNA Profile", 7 January, 2008, available at: http://www.theregister.co.uk/2008/01/07/delete_your_dna_profile/ .

[140] Nuffield Report, *supra* note 3 at s. 4.38.

[141] Christopher Hope "DNA Profiles of one million innocent people should be erased, watchdog says", July 30, 2008, available at: http://www.telegraph.co.uk/news/newstopics/politics/2471425/DNA-profiles-of-one-million-innocent-people-should-be-erased-watchdog-says.html.

[142] *Id.*

[143] *Youth Criminal Justice Act*, (2002, c.1) at s. 120(3) and 128(3); OPC Interview, *supra* note 20.

By contrast, according to the Home Office, the United Kingdom's National DNA Databank contains the profiles of 39, 095 children between the ages of 10-17 who have never been "convicted, cautioned, received a final warning/reprimand and had no charge pending against them."[144] Additionally, the Home Office has confirmed that profiles of 49 children aged nine or under are also on the database. This is especially noteworthy since in England and Wales, only children aged ten and over may be held criminally responsible.[145] There has even been a suggestion by police that DNA be taken from children who show "potential" for criminal/anti-social behaviour, at the discretion of their teachers.[146] The Human Genetics Commission found that "the DNA profile of a child convicted of a minor offence should be retained for a limited period of time", preferably no more than 5 years,[147] an approach which would be closer to that of Canada.

The creation of a nation-wide DNA databank is currently under consideration in the UK.[148] The legality of such an endeavour, which would require the retention of DNA data related to those never convicted of an office, will depend heavily on the outcome of a case currently at the European Court of Human Rights (ECtHR). The case has been ruled admissible,[149] but at as of the date of writing this paper the ECtHR has not yet rendered a decision. The complaint comes from two individuals who were arrested for recordable offences. DNA samples and fingerprints were taken, but they were ultimately never convicted. They requested that their DNA samples and fingerprints be destroyed, which was refused by the government. Their case at the ECtHR claims that the retention of their fingerprints, DNA samples and DNA profiles and their continuing use in investigations

[144] Christopher Hope, Telegraph, "Profiles of 40,000 innocent children on DNA database", August 15, 2008, available at: http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/2565016/Profiles-of-40000-innocent-children-on-DNA-database.html.
[145] *Id.*
[146] *See:* Mark Townsend and Anushka Asthana, The Guardian, "Put young children on DNA list, urge police", March 16, 2008, available at: http://www.guardian.co.uk/society/2008/mar/16/youthjustice.children.
[147] *Supra* note 141.
[148] Nuffield Report, *supra* note 3 at 4.73.
[149] *S. & Michael Marper v. The United Kingdom*, Application nos. 30562/04 and 30566/04 Decision on Admissibility [hereinafter "Marper"].

constitutes violations of articles 8 (respect for private life) and 14 (discriminatory treatment) of the European Convention on Human Rights.[150] Their claims were rejected by national courts, with the House of Lords relying on statistical evidence showing the number of crimes linked to individuals already on the database.[151]

In the House of Lords decision,[152] Lord Steyn held that the legislative framework provided enough comfort as to the retained information, claiming that the retention of such bioinformation would only affect individuals as it ever matches samples from a crime scene.[153] Finally, he rejected any difference between the retention of DNA profiles and DNA samples in respect of the claims at issue.[154] Lord Steyn holding that the retention of fingerprints and DNA samples did not constitute an interference with convention rights to private life, but if this were wrong, the interference would only be "modest".[155] The effect of this decision by the ECtHR once a judgment is rendered will be far-reaching in the United Kingdom in terms of the legislative and policy implications of a finding that retention of innocent persons' DNA samples or profiles is a violation of the Convention. Likewise, a finding that there is no violation may open the doors to more a more inclusive National DNA Database, with a government empowered in its mandate by any such finding.

It is relevant to a consideration of the issues in the pending Marper decision that the Council of Europe's Recommendation No. R (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system[156] shows that the Council of Europe's position appears to favour destruction once DNA materials are no longer required for the purpose for which they were collected. The Explanatory

[150] *Id.* at 8.
[151] *Id.* at 3.
[152] *Supra* note 44
[153] Marper, *supra* note 149 at 4; Marper – House of Lords, *supra* note 44 at para. 37.
[154] Marper, *id.* at 5; Marper – House of Lords at *supra* note 44 at prar. 41.
[155] Marper, *id.* at 4; Marper House of Lords, *supra* note 44 at para 31.
[156] (Adopted by the Committee of Ministers on 10 February 1992
at the 470th meeting of the Ministers' Deputies), as cited in Marper, *supra* note 149 at 7-8.

Memorandum to the Recommendation,[157] adds 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 offenders, the data should be deleted once persons have been cleared of suspicion."[158] This approach does not appear to support the retention of innocent individuals for speculative searches in the future, as is permitted in the United Kingdom's system.

2.7 Chapter Conclusions

In this Chapter, the forensic DNA databank regimes' requirements and processes for the collection of DNA samples in Canada and the United Kingdom were reviewed and compared. It was demonstrated that in terms of threshold of offences, timing in criminal justice process and judicial oversight required, the process in the United Kingdom promotes the collection of DNA samples in a wider range of circumstances than that in Canada. Likewise, in respect of retention of DNA samples and their related DNA profiles, the United Kingdom falls on the side of inclusion moreso than in Canada. While in Canada DNA samples and profiles may only be retained in respect of individuals actually convicted of a specific offense, in the United Kingdom, those so much as arrested for an offence (and in the United Kingdom, a broader range of offences carry with them the right to take a DNA sample) will have their DNA profiles kept on record for the rest of their lives. As will be examined further in Chapters 3 and 4 below, the threshold for inclusion and retention of an individual's data in a DNA databank has implications for the range of individuals in respect of whom any data protection risk affects. In Chapter 3, this paper will turn to the legislative regimes surrounding the uses which can be made of DNA data retained as described in this Chapter 2.

[157] (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the ministers' deputies).
[158] *Id.* at para. 49.

CHAPTER 3 –

REGULATING USE FOLLOWING COLLECTION

In Chapter 2 the process of collecting DNA samples and the applicable regulations related to doing so were reviewed and compared. This Chapter 3 contains a discussion and comparison of how DNA is regulated *following* its collection and retention. In this Chapter, restrictions on secondary uses and disclosure are examined.

3.1 Avoidance Of Secondary Uses

To the extent that DNA samples or DNA profiles are legally retained, various legislative, operational and technical measures can be used to attempt to curb unauthorized or secondary uses of them. Below an overview of the legal requirements for such measures in Canada and the United Kingdom are provided. The effectiveness of these methods in practice will be further examined in Chapter 4.

3.1.1 Canada

One method used in both Canadian and United Kingdom legislation with a view to deterring use of DNA samples for secondary purposes is the creation of legislative prohibitions on the use of the samples for purposes other than the forensic investigative or DNA matching for which it was collected. The Canadian *Criminal Code* prohibits the use of DNA samples other than "for the purpose of forensic DNA analysis in the course of an investigation of a designated offence".[159] The *DNA Identification Act*'s governing principles include respecting the interest of protecting society and the administration of justice through the use of DNA profiles, as well as the principle that neither DNA profiles or samples should be used for any purpose other than law enforcement in accordance with the Act.[160] The third and final principle of the Act is to place safeguards on the handling of DNA profiles and

[159] *Criminal Code*, *supra* note 57 at s. 487.08(1).
[160] *DNA Identification Act*, *supra* note 56 at ss. 4(a) and (b).

DNA samples in order "to protect the privacy of individuals with respect to personal information about themselves".[161] The same Act prohibits the sharing or use of DNA samples for any purpose other than forensic DNA analysis.[162]

The Supreme Court of Canada has examined the scope of the definition of "Forensic DNA analysis" in respect of which uses of the DNA sample are permitted in the context of carrying out testing on it, and found that that:

> 'forensic DNA analysis' is defined […] as the comparison of the DNA of the bodily substance from a person in execution of a warrant with the results of the DNA [of the crime scene sample]. The definition also includes "any incidental tests associated with that analysis". The exact scope of these incidental tests remains for future cases to determine. However, I am inclined to believe […] that what is authorized is simply the furtherance of the "forensic DNA analysis". That is, those tests that may be useful in advancing the matching of the two samples, and nothing more, are permitted. Furthermore, the results of such DNA analysis may only be used in the course of an investigation of the designated offence."[163]

This statement by the Supreme Court of Canada makes clear that DNA samples are not to be tested for anything beyond what is necessary for matching samples.

Regarding the use of DNA profiles created from the DNA samples, the Criminal Code states that the results of a forensic DNA analysis (i.e. the DNA profile) obtained by warrant may not be used other than in the course of investigating the designated offence in respect of which the warrant was issued or bodily substance found at a crime scene, or related proceedings.[164] An additional layer of protection is created by the fact that the Criminal Code makes the breach of the above provisions a criminal offence.[165]

Likewise, the *DNA Identification Act*, has as one of its principles that DNA samples and DNA profiles "may only be used for law enforcement purposes in accordance with this Act, and not for any unauthorized purpose."[166] As a general rule, it states that no one may use

[161] *Id.* at s. 4(c).
[162] Id. at s. 10(5).
[163] *R.* v. *S.A.B.*, *supra* note 50 at para 13.
[164] Criminal Code, *supra* note 57 at s. 487.08(2).
[165] *Id.* at s. 487.08(3) and (4) and *R v. S.A.B., supra* note 50 at para. 50.
[166] DNA Identification Act, *supra* note 56 at s. 4(b).

DNA profiles except in accordance with the *DNA Identification Act.*[167] Further it prohibits sharing information stored in the National DNA Data Bank other than access granted by the RCMP Commissioner for the purposes of operating and maintaining the databank, or for training purposes.[168]

Although limitations on use are seen as positive from a data protection perspective, it is noteworthy that these limitations can also hinder uses of the DNA databank that might have meritorious purposes. For example, in Canada, the National DNA Data Bank may not be accessed for the purpose of identifying missing persons. This is another issue that is expected to be raised in the overdue five-year review of the DNA Identification Act, when it is held.[169]

3.1.2 United Kingdom

As noted above, the legislative framework in the United Kingdom is based on a series of legislative amendments to a large number of Acts broadening the scope of when police may collect and retain DNA samples and profiles. By contrast, the legislation is more efficient in its restrictions on use. Quite simply, The Police and Criminal Evidence Act, 1984 states that that DNA samples, unless they were taken from a person who was not suspected of the offence,[170] can be retained after the fulfillment of the purpose they were taken for, but can only be used for the purposes of "prevention or detection of crime, the investigation of an offence or the conduct of a prosecution."[171] As was noted above, the National DNA Data Base is not itself regulated by statute, rather the handling of samples and information derived therefrom[172] are discussed generally in legislation.

[167] *Id.* at s. 6(6).
[168] *Id.* at s. 6(7) and s.7(a) and (b).
[169] NDDB Interview, *supra* note 123.
[170] PACE, *supra* note 64 at 64(3).
[171] *Id.* at s. 64(1A); also see Nuffield Report, note 3 at s. 6.2.
[172] PACE, *supra* note 64 at s. 64(1A).

More specific regulation comes from outside of the United Kingdom. For example, the type of restriction intended to temper secondary uses of DNA samples is seen in the Council of Europe's "Recommendation on the Protection of Medical Data", Principle 4.8 of which states, with respect to forensic DNA analysis that "[t]he data should only be used to establish whether there is a genetic link in the framework of adducing evidence, to prevent a real danger or to suppress a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically."[173]

At the European level, on May 27, 2005, a treaty "on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration"[174] was signed between seven EU member states countries (Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain) at Prüm, Germany (the "Prüm Treaty"). On September 17, 2007, the Council Decision on the Stepping up of Cross-Border Cooperation, Particularly in Combating Terrorism and Cross-Border Crime[175] (hereinafter the "Council Decision") in effect codified the Prüm Treaty into EU law. Article 29 of the Council Decision sets out that the automated search procedure must include state-of-the-art technical measures "to ensure data protection and data security, in particular data confidentiality and integrity" as well as technical measures for encryption and measures to ensure that [certain searches] can be checked.[176]

Despite the legislative prohibitions and creation of criminal sanctions for their violation, critics such as the Innocence Project organization suggest that mistakes and abuses will occur nonetheless.[177] For this reason, proactive operational procedures and internal checks are also required, rather than simply prohibitions which only provide retroactive

[173] Council of Europe, "Recommendation on the Protection of Medical Data", cited in Nuffield Report, *supra* note 12 at s. 2.21.
[174] Brussels, 7 July 2005 (28.07).
[175] 11896/07, Council of the European Union, Brussels 17 September 2007 [hereinafter "Council Decision"].
[176] *Id.* at s. 29(2).
[177] Innocence Project, online at: http://innocenceproject.org/.

punishment. This concept is recognized in the language of Canada's DNA Identification Act, where it requires that safeguards be placed on the use and communication of, and access to DNA profiles and DNA samples.[178] The types of safeguards that the Canadian National DNA Data Bank has put in place include those discussed above[179] which separate the DNA profile, DNA sample and any personally identifiable information both operationally and physically.

3.2 Familial Searches

Where a perfect match is not found, but it is close (e.g. not all loci match, but only a close match is found) the similar DNA profile tells police that the true perpetrator may be someone related to that individual.[180] In such a case, police may wish to seek DNA from a member of the individual's family. This, of course, raises issues of privacy for the family members whose genetic information is then brought into the system, whether known (i.e. if a sample is requested) or unbeknownst (i.e. a discarded tissue is used to take a DNA sample) to them.

3.2.1 Canada

Familial searches are not permitted in Canada. In Canada the governing legislation applies only where there is a true match (e.g. all loci match). Where there is less than a full match, a DNA profile cannot be linked back to the name of the individual to whom it relates and therefore, no family can be contacted.[181]

3.2.2 United Kingdom

By contrast, familial searches are permitted in the United Kingdom only in limited circumstances. In compiling their comprehensive report, the Nuffield Council on Bioethics

[178] DNA Identification Act, *supra* note 56 at s. 4(c).
[179] See *supra* at s.2.5.1.
[180] See e.g. Nuffield Report, *supra* note 3 at 6.6.
[181] OPC Interview, *supra* note 20.

were told by the Association of Chief Police Officers that the circumstances under which it is permitted were "operationally sensitive", leaving the question unanswered. It is known, however, that the success of familial searches is rare, given the number of unsuccessful partial matches that they are bound to produce.[182]

3.3 Sharing DNA Profiles And Samples With Other Countries

3.3.1 Canada

The Canadian *DNA Identification Act* sets out the conditions under which Canada's law enforcement agency, the RCMP, may share DNA profiles in its possession with foreign law enforcement agencies, both upon the request of a foreign law enforcement agency and upon a request originating in Canada. When Canada receives a DNA profile from a foreign government or international organization, the Commissioner "may" compare the profile to those in Canada's DNA data bank to look for a match.[183] The Commissioner is then authorized (note the language is permissive, not mandatory) to share the following information with the requesting state or organization:

> (a) if the DNA profile is not already contained in the data bank, the fact that it is not;
>
> (b) if the DNA profile is already contained in the data bank, the information contained in the data bank in relation to that DNA profile; and
>
> (c) if the DNA profile is, in the opinion of the Commissioner, similar to one that is already contained in the data bank, the similar DNA profile;[184]

Further, if the foreign state's subsequent comparison of the similar profile provided pursuant to (c), above, does not exclude that individual as a possible match, the RCMP Commissioner may provide the information related to that similar DNA profile contained in Canada's databank.[185] It is noteworthy that the identity of the individual to whom the DNA profile

[182] Nuffield Report, *supra* note 3 at s. 6.6.
[183] DNA Identification Act, *supra* note 56 at s. 6(3).
[184] *Id.* at s. 6(1) (a) – (c), as referred to in s. 6(3)(a).
[185] *Id.* at s. 6(3) (b).

relates is only provided where there is a match, but not in case (c) above, or where the individual does not match, but cannot be excluded by a foreign state as a possible match.[186]

In the case of a Canadian law enforcement agency investigating an offence designated as a primary or secondary offence, on their request, the RCMP Commissioner can share a DNA profile held in the crime scene index with "the government of a foreign state, an international organization established by the governments of states or an institution of any such government or international organization."[187]

The *DNA Identification Act* sets limitations on when Canada may communicate DNA profiles and/or related information, whether upon a foreign request or a request from Canada to a foreign government or institution. For either of these types of communications of personal information, the Canadian government or a related institution must have entered into an agreement or arrangement with the relevant foreign government, organization or institution "authorizing the communication solely for the purposes of the investigation or prosecution of a criminal offence."[188] This echoes Canada's *Privacy Act*, which authorizes the disclosure of personal information held by the government upon entering into an agreement or arrangement with "the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation."[189] Canada's Office of the Privacy Commissioner has been advocating reforms to the *Privacy Act* that would require that such international agreements impose specific obligations on the country or institution receiving information from Canada.[190]

[186] OPC Interview, *supra* note 20.
[187] DNA Identification Act, *supra* note 56 at s. 6(4).
[188] *Id.* at s. 6(5).
[189] *Supra* note 58 at s. 8(2)(f).
[190] OPC Interview, *supra* note 20.

Such reciprocal obligations are important because, as was noted in *R. v. T.T.*,[191] otherwise the provisions on destruction of DNA profiles in the DNA Identification Act would lose their meaning. As the court held,

> [i]t would be of little use for our country to destroy a young offender's DNA profile after we've sent copies to DNA data banks in the United States and other foreign governments.. So the discretion exists to simply send all of our young offender profiles to another Country just before the time limit within which the statute says they must be destroyed and avoid complying with privacy protection of young persons pursuant to the [Youth Criminal Justice Act, which requires the earlier destruction of DNA profiles of offenders under 18 years of age].[192]

Sharing done through the procedures described above are carried out through Interpol. No other country has direct access to Canada's National DNA Data Bank or the information stored on it.

3.3.2 United Kingdom

At a national level, DNA profiles are shared with other countries under an exception in the United Kingdom's *Data Protection Act*,[193] which permits an exception to that Act's non-disclosure principles where information is being shared in respect of crime prevention,[194] but is not dealt with in depth in any significant way.[195] At the European level, the Council Decision, as the Prüm Treaty did, sets out requirements for Member States with respect to, *inter alia*, sharing of DNA data. The general premise is set out in respect of the mutual access provisions in the course of a criminal investigation, as follows:

> Member States shall allow other Member States' national contact points as referred to in Article 6, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Searches may be conducted only in individual cases and in compliance with the requesting Member State's national law.[196]

With respect to retention and deletion of data obtained from other Member States and the obligations of other Member States who obtain data from the United Kingdom, the

[191] [2001] O.J. No. 2936 [hereinafter *R. v. T.T.*].
[192] *Id.* at para. 60.
[193] 1998 CHAPTER 29.
[194] *Id.* at s. 29.
[195] Nuffield Report, *supra* note 3 at 7.47.
[196] Council Decision, *supra* note 175 at art. 3(1).

Council Decision requires that Member States delete personal data: (i) which should not have been supplied to or received by it; (ii) when no longer necessary for the purpose for which it was supplied; and (iii) in accordance with the national law in the supplying member state as to the maximum retention period (of which it must inform the receiving state at the time), unless it would be prejudicial to the individual involved to delete his or her data, in which case it must be blocked from access instead.[197] The reference to the national law of the supplying member state will temper the ability of the United Kingdom to retain samples it receives through this process, as it may receive samples from States with retention policies which favour destruction more than that of the United Kingdom.

The Council Decision states that "reference data" from national DNA databanks is to be made available to the appropriate agents from other States.[198] Such reference data includes only "DNA profiles established from the non-coding part of DNA and a reference number [and] [r]eference data shall not contain any data from which the subject can be directly identified."[199] Upon finding a match between the requesting State's DNA profile and a DNA profile supplied by another State, the provision of "further available personal data and other information relating to the reference data" is to be governed by national law of the requested Member State.[200] This means that DNA *samples* themselves may not be shared, rather only DNA profiles which do not identify the individual. This is similar to the Canadian system for sharing internationally and reduces the potential exposure to data protection risks based on the sharing of DNA data in the criminal context with other states.

The Council Decision requires member States to allow a designated contact from any other member state access to reference data in a manner permitting automated searches to

[197] *Id.* at s. 28(3).
[198] *Id.* at s. 3(1).
[199] *Id.* at art. 2.
[200] *Id.* at art. 5.

compare DNA profiles.[201] "Automated Search Procedure" is defined in the document as "direct access to the automated files of another body where the response to the search procedure is fully automated."[202] Such access is limited to individual cases only,[203] which reduces the type of broad speculative searches that could be open to abuse or expansion to searching for purposes beyond individual forensic investigations.

If the automated search results in a match, the reference data is to be automatically provided to the requesting state (Ch. 2, art. 3(2), or an automatic notification of no match being found.[204] The Council Decision further sets out that States will compare their unidentified DNA profiles with the reference data from other States, in accordance with the providing State's national law.[205] A difference is seen here between the Canadian and European regimes. International sharing of DNA profiles and related information by Canada is done through Interpol, there is no direct or automated foreign access to Canada's National DNA Data Bank.

The Council Decision's regime for sharing personal information related to DNA profiles accounts for data protection issues in several ways. The first means of protecting personal data is the limited scope of circumstances in which personal information related to the reference data can be provided, used and retained. No personal data is to be supplied until the provisions of the Decision regulating the conditions are implemented in national law of a Member State to the satisfaction of the Council, other than in respect of the original parties to the Prüm Treaty (which did not include the UK).[206]

Processing of DNA profile data is only permitted to: (i) determine whether there is a match; (ii) if there is a match, to "prepare and submit a police or judicial request for legal

[201] *Id.* at art. 3.
[202] *Id.* at s. 24(1)(b).
[203] *Id.* at s. 3(1).
[204] *Id.* at art. 3.
[205] *Id.* art. 4.
[206] *Id.*at s. 25(3).

assistance in accordance with national law"; and (iii) to record the data in accordance with the Council Decision.[207] The Council decision also permits a requested State to take a DNA sample from a particular individual in its territory and provide a DNA profile to the requesting State where there is an ongoing investigation and no DNA profile is available for that individual.[208] Such a request, for collection of DNA must, however, meet the requirements for the issuance of a warrant in the requesting Member State and the requirements for collection and examination of the Sample in the requested Member State.[209] These requirements will limit the scope of application of this power to request that another State take a sample from a person in its territory. In the case of the United Kingdom, for example, only a country that had as low a threshold for collection in respect of severity of offences as the United Kingdom does, could request a sample be taken in respect of some of the lesser Recordable Offences. Restrictions on use and protection of data are set out where the Council Decision states that personal data may not be processed by a receiving state other than for the purposes, in accordance with the Council Decision, for which the data was supplied.[210] Any other processing of such data is only permissible: (i) with the prior approval of the state administering the file and subject to the laws of the receiving state. [211]

The recognition by the Council Decision of the significance of sharing DNA reference data is seen in the terms related to sharing of personal data in respect of potential terrorist activities. Where circumstances give rise to a belief that an individual may commit a terrorist offence, a Member State may provide "surname, first names, date and place of birth" and details of the circumstances described above."[212] It is noteworthy that DNA cannot be

[207] *Id.* s. 26(2).
[208] *Id.* art. 7.
[209] *Id.*
[210] *Id.* at s. 26(1).
[211] *Id.*
[212] *Id.* at ss. 16(1) and (2).

provided in a similar manner in such circumstances, rather it is governed by the provisions discussed above such that it could be used retroactively, but not speculatively.

The Council Decision sets out levels of data protection required for any data supplied pursuant to the same Decision. Member States' national laws must "guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol of 8 November 2001 and in doing so, shall take account of Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe to the Member States regulating the use of personal data in the police sector, also where data are not processed automatically."[213]

Despite the references to data protection standards in the Council Decision, concerns have been raised as to whether the issue is sufficiently dealt with. In general, the fact that this decision falls within the area of "police and judicial cooperation in criminal matters", which is exempted from the *Data Protection Directive*, led to concerns that the issue of data protection needs to be more thoroughly dealt with in respect of this so-called 3rd pillar. Likewise, the European Data Protection Supervisor (EDPS), Peter Hustinx, has expressed concern that in the final draft of the Council Decision, the "Council has not sufficiently taken my remarks into account"[214] He noted that "[t]here will for instance be a lot of variation in the level of data protection afforded by different member states as the decision does not harmonise it, but relies very much on national law."[215] As noted above, in the instances where a country with a broader collection and retention policy is the requesting State it may have an impact on the requested State, insofar as the Council Decision makes certain processing requests contingent on meeting the national law of the requesting (as opposed to

[213] *Id.* at s. 25(1).
[214] "Police will share data across Europe against privacy chief's advice" OUT-LAW News, 14/06/2007, available at: http://www.out-law.com//default.aspx?page=8148.
[215] *Id.*

the requested) State. However, as noted above, the same holds true insofar as more stringent requirements of other States may limit what the United Kingdom is able to ask of them.

3.4 Chapter Conclusions

This Chapter examined the legislative measures taken to protect DNA data in the hands of the State. Both Canada and the United Kingdom have legislative terms in place which limit the purposes for which DNA samples and profiles may be used. The regime in the United Kingdom is also affected at the international level by its participation in the European Union and the application of E.U. laws, and in particular the Council Decision codifying the Prüm Treaty. While this does facilitate the circumstances under which DNA data collected by the United Kingdom may be shared outside of its borders, or DNA samples taken from its citizens to assist other State's investigations, the Council Decision's procedures are arguably stronger in respect of data protection than those of the United Kingdom (leading to the conclusion that the outcome would be worse in net effect for E.U. members other than the United Kingdom, an issue which is beyond the scope of this paper). In Chapter 4, this paper will now turn to risks existing in respect of the DNA data retained by States, which have been shown to be set at differing thresholds for collection and similar restrictions on use in Canada and the United Kingdom. The implications of these risks in each of these types of regimes will be discussed next.

CHAPTER 4 –

DATA PROTECTION ISSUES

In this Chapter, issues related to data protection in the two national forensic DNA databank regimes discussed in Chapters 2 and 3 will be reviewed and the two regimes' methods of dealing with them will be compared. The breadth of both Canada's and the United Kingdom's forensic DNA databank regimes has been expanding in recent years in a piecemeal fashion as discussed above in this paper,[216] the United Kingdom's even moreso than Canada's. Such expansion means that more people, with less of an involvement or connection to serious (or any) crime, are being put onto national DNA databanks. In response to this trend, questions are being raised regarding the appropriate balance between a desirable increase in resolving crimes and obtaining convictions versus respecting and protecting individuals' rights with respect to their bioinformation. Below, the history of these expansions as well as the data protection implications raised by critics of this expansion will be discussed.

Next, the issue of whether having a more inclusive databank in fact leads to more convictions will be examined. If the increase in interference with and risk to the protection of personal information is not matched by a proportionate increase in effectiveness of the databank, then this rationale for collecting and retaining personal bioinformation from a greater number people will be a questionable justification. Finally, the data protection risks which exist in respect of DNA profiles and DNA samples which are held in government hands will be examined and the approaches taken by each of Canada and the United Kingdom in response to these problems will be addressed and a recommended approach will be proposed.

[216] See *supra* Chapter 2.

4.1 The Expansion of Forensic DNA Databanks

Compelling arguments have been made on both sides of the debate over the expansion of DNA databanks to include more individuals. Expansion is done through broadening the categories of individuals for whom a DNA sample is taken and the circumstances in which it, and/or a related DNA profile is retained in the DNA databank. The argument in favour of expansion was articulated by Lord Steyn in his decision in Marper, where he justified any interference with the privacy of individuals held on the DNA Database who had not been convicted of an offence as it being "in the public interest in its fight against crime for the police to have as large a database as possible."[217]

4.1.1 DNA Databank Expansion in Canada

In Canada, the list of offences included in the definition of "designated offences" (offences for which a DNA sample may be taken for inclusion in the National DNA Data Bank) was expanded by amendments to the Criminal Code in 2005, which came into effect on January 1, 2008.[218] The amendments created additional designated offences, thereby expanding the breadth of offences in respect of which DNA samples may be taken and also reclassified certain secondary designated offences as primary designated offences.[219]

At the time these amendments were being proposed, Canada's Privacy Commissioner expressed concern about the expansion, noting that "[w]e believe that, in principle, the number of offences for which DNA samples can be taken and included in the Data Bank should be kept to a minimum, and that the inclusion of offences must be based on a clearly articulated and demonstrably justifiable rationale."[220] The original rationale proposed for the collection of DNA for a national forensic DNA data bank in Canada was based on the

[217] Marper – House of Lords, *supra* note 152 at para. 39.
[218] An Act to amend certain Acts in relation to DNA identification (2007, C-22); An Act to amend the Criminal Code, the DNA Identification Act and the National Defence Act (S.C. 2005, c.25); see also Frederico & Rondinelli's DNA Netletter, March 1, 2008, issue #98.
[219] *Id.*
[220] Statement given to the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, February 8, 2005, http://www.privcom.gc.ca/speech/2005/sp-d_050208_e.asp.

following two considerations: "the serious nature of the offence and the likelihood that DNA samples would be found at the crime scene."[221] The Supreme Court of Canada confirmed this sentiment in the *R. v. S.A.B*. case, that the forensic DNA Databank regime only applies to designed offences "which consist primarily of violent and sexual offences that might involve the loss or exchange of bodily substances that could be used to identify the perpetrator through DNA analysis."[222] With this original rationale in mind, the Privacy Commissioner of Canada noted, in response to the proposed expansion in 2005:

> We have seen a fundamental shift away from this rationale toward what appears to a growing national registry of convicted criminals. This is a marked move away from the underlying philosophy of the DNA Data Bank scheme as it was originally conceived and approved by Parliament. New offences were added with the adoption of then Bill C-36, the Anti-Terrorism Act, in 2001 and more offences are now being proposed […] that do not appear to meet these criteria of violent and sexual offences involving the loss or exchange of bodily substances.[223]

Reflecting this same concern that the government is no longer relying on the original logic of the DNA databank scheme to justify the addition of new offences, in an interview with a Senior Policy Analyst from the Commissioner's office, he noted that the *Anti-Terrorism Act* offences recently added include those for which a DNA sample would not be an effective investigative tool, such as terrorist financing offences.[224] The addition of offences such as this one is said to go against the original logic of only adding offences where the offender would leave a bodily sample at the crime scene.[225]

The concerns of the Canadian Privacy Commissioner and her Office's official positions can be contrasted with those of law enforcement representatives in Canada, who favour the approach of the United Kingdom. The Privacy Commissioner's Office has acknowledged that the more inclusive system in the United Kingdom is seen by law

[221] *Id.*, citing the Honourable Andy Scott, appearing before the same Committee on February 4, 1998.
[222] *Supra*, note 50 at para. 19.
[223] *Supra* note 220.
[224] OPC Interview, *supra* note 20.
[225] *Id.*

enforcement officials as ideal.[226] The former Chief of Police of Toronto, Julian Fontino, who was quoted as saying that in his opinion, DNA samples should be able to be collected from anyone arrested.[227] Current Toronto police chief Bill Blair was also quoted as saying that he hopes that by the year 2011 Canadian police will be able to collect DNA from anyone charged, not just convicted, of an offence.[228] According to the Commissioner's Office, the idealism of the UK system by law enforcement has made the task of limiting expansion more difficult for privacy advocates in Canada.[229]

4.1.2 DNA Databank Expansion in the United Kingdom

In the United Kingdom, the "DNA Expansion Programme" was implemented in the United Kingdom in the year 2000 following a commitment by the then-Prime Minister to provide funding to get every offender on the DNA Database. In the first 5 years of the Expansion Program, over 2,250,000 people's DNA samples were taken and profiles added to the Database, triple the number than had been added in the previous five years.[230] It was reported that in 2006-2007 DNA profiles were being added to the DNA Database at the equivalent of 76 new profiles per hour.[231] The Programme was seen as a success[232] and has fueled proposals for even further expansion. The Home Office proposed in March, 2007 that the category of a "recordable offence" be removed and DNA samples be taken from anyone arrested for *any* offence.[233] The Nuffield Council on Bioethics calculated that this would potentially reach 25 percent of the male and seven percent of the female population of the

[226] *Id.*
[227] Toronto Star,19 October 2004, p. B2, cited in Parliamentary commentary to Bill C-13. Available at: http://www.parl.gc.ca/common/Bills_ls.asp?Parl=38&Ses=1&ls=C13 - 15.
[228] Rick Westhead, "Widen DNA Dragnet: Blair", April 12, 2008, available at: http://www.thestar.com/News/GTA/article/413851.
[229] *Id.*
[230] Reporting Achievement, *supra* note 71 at 4.
[231] Andy Bloxham, "DNA bank solves one crime per 800 profiles", May 6, 2008, available at http://www.telegraph.co.uk/news/uknews/1929849/DNA-bank-solves-one-crime-per-800-profiles.html. However, the number of crimes detected only rose by 839 to 41,148.
[232] *Id.*
[233] Nuffield Report, *supra* note 3 at s. 1.24

United Kingdom.[234] Other proposals from the United Kingdom have suggested taking DNA from children who show "potential" for criminal or anti-social behaviour[235] and proposals by the Home Office include the creation of a nation-wide DNA databank[236] and even take the DNA of all visitors to the country.[237]

Equally in contrast to the Canadian regime's minimalist approach as that of the United Kingdom, the Council of Europe Recommendation R (92) 1 *on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system* (1992) states at s. 5 that "Recourse to DNA analysis should be permissible in all appropriate cases, independent of the degree of seriousness of the offence."[238] This is reflected in the United Kingdom's approach to use of its DNA database.

4.1.3 Comments and Recommendations

While Canada's expansion has been slower than that in the United Kingdom, it appears to be moving in the direction of expansion. Canada's Privacy Commissioner, as discussed above, has expressed concern regarding the need to continue to limit the DNA databank to its original purposes and collect and retain DNA samples and profiles in accordance with that framework. The approach in the United Kingdom is still much more extensive and inclusive than that in Canada, but illustrates some of what the future holds if Canada continues in this direction.

One argument, as put forward by Michael Smith, suggests that rather than continuing on the piecemeal expansion of who the DNA databank covers, as seen in both Canada and the United Kingdom, a national DNA databank policy should "approach that coverage

[234] *Id.*
[235] *Supra* note 146.
[236] See e.g. James Orr, "Judge wants everyone in UK on DNA database", September 5, 2007, available at: http://www.guardian.co.uk/uk/2007/sep/05/humanrights.ukcrime.
[237] Nigel Morris, "A 'chilling' proposal for a universal DNA database", September 6, 2007, available at: http://www.independent.co.uk/news/uk/crime/a-chilling-proposal-for-a-universal-dna-database-401503.html.
[238] Recommendation R (92) 1 *on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system* (1992). See also Nuffield Report, *supra* note 3 at Appendix 3.

deliberately--not piecemeal."[239] He argues that expanding the DNA databank "as politics permits or requires, to more and more categories of individuals involved in the criminal justice system--turns out to be an expensive way to create a DNA database covering a very great (and racially skewed) portion of the population."[240] He concludes that a DNA databank covering all of the population would be more efficient and focus on all individuals equally rather than focus only on the groups over-represented on the databank at any given time.[241]

From a privacy, perspective, however, an all-population DNA databank would not be the recommended approach, regardless of its balancing out other issues such as discrimination. An all-inclusive NDA databank would require, by its definition, the collection of DNA from those who have never had so much as a brush with the law and certainly have not been convicted of any offence, of any severity. Both Canada's Privacy Commissioner and the Nuffield Council have expressed concern about the risk of police having the power to take DNA in respect of offences that do not relate to DNA evidence.[242] The Nuffield Council argue that once the threshold for police being permitted to take a DNA sample are low enough, greater oversight would be needed "to ensure that arrests could never be made simply for the purpose of 'speculatively' obtaining bioinformation."[243] It has also been argued that

> Allowing the government to maintain a database of every individual's genetic information creates, at the very least, a government that knows more about its citizens. Even if the information is limited to identifying fingerprints, genetic or traditional, without more intrusion into the private thoughts and minds of individuals, there is still something ominous and oppressive about an all-knowing state. The inherent danger to our conception of ourselves as a free and autonomous society requires that further expansion of the preventive state, represented by the creation of a universal database, be vigorously opposed.[244]

[239] Smith, *supra* note 129 at 99.
[240] *Id.* at 99-100.
[241] *Id.* at 100.
[242] Presentation to the Standing Committee on Justice and Human Rights, Bruce Phillips, (February 12, 1998), available at: http://www.privcom.gc.ca/speech/archive/02_05_a_980212_e.asp and Nuffield Report, *supra* note 3 at s. 4.18.
[243] Nuffield Report, *supra* note 3 at s. 4.18.
[244] Peterson, *supra* note 15 at 1237-8.

The reference to freedom is reminiscent of the arguments made in the name of prioritizing liberty in Chapter 1 - privacy-friendly arguments would suggest that the government should justify why DNA collection in a particular case is justified. Where it is used for investigatory or evidentiary purposes it may be easier for a government to meet this burden, than when it seeks to collect DNA in respect of crimes for which DNA evidence would not be part of the prosecution, or to retain DNA of someone who was ultimately not convicted of the offence. In such a case, the burden on justifying the collection should remain with the government, not the citizen.[245]

Following the initial collection, the approach most favouring data protection would appear to be one that only retains DNA samples relating to individuals who have been convicted of crimes for which DNA evidence would be relevant to the crime. In this respect, the Canadian National DNA Data Bank is more data-protection-friendly than the United Kingdom's National DNA Database. The Canadian approach is, however, moving in the direction of expansion in the piecemeal fashion discussed above. Based on the discussion above, the trend towards expansion of forensic DNA databanks begs the question of whether a bigger DNA databank is necessarily a better one. This answer to this question must then be viewed in light of the implications of any such expansion in law.

4.2 Does a Bigger Databank mean a Better Databank?

4.2.1 The Arguments and Evidence

It is argued that solving crimes and conviction of offenders has been facilitated by law enforcement agencies having access to a growing databank of DNA profiles kept on record against which to match new and unidentified samples. The argument made in favour of expanding forensic DNA databanks is that the bigger it is, the better, since there will be more matches between crime scene samples and profiles in the databank of an individual who

[245] See *supra* at ss. 1.4 and 1.5.

might not have otherwise been found as a suspect.[246] This is seen as a triumph for law enforcement.[247] The correlation between a more inclusive DNA databank and a more efficient DNA databank, however, has been challenged by those who argue that any perceived benefits are questionable and, in any case, significant enough to justify the greater intrusion in privacy. Simoncelli argues that "a comprehensive assessment of the value of a data bank to society must carefully weigh any benefits of this tool to law enforcement against its social and financial costs."[248]

In support of its claim that taking DNA samples for less serious crimes assists law enforcement in respect of more serious crimes, in its 2006-2007 annual report on the National DNA Data Bank, the Royal Canadian Mounted Police ("RCMP") states that "there are no minor crimes for the [National NDA Data Bank]."[249] The United Kingdom's Home Office similarly notes that it often catches serious offenders when they give a DNA sample in respect of a minor offence commit at a later date.[250] The RCMP's annual report notes that between 12% - 15% of all hits in investigations for primary offences, come from a match between an individual put into the DNA Data Bank for a secondary offence and the report therefore concludes that "entering DNA profiles from secondary offences often leads to breaks in solving more serious crime."[251] It is noteworthy that the report does not state which crimes, other than break and enter, itself already relatively violent in nature, are seen as correlated to the later commission of primary designated offences. A justification for collecting DNA samples in respect of more minor offences based on a correlation between the commission of that offence and the later commission of more serious offences should,

[246] See e.g. Reporting Achievement, *supra* note 71 at para. 1.
[247] Simoncelli, *supra* note 34 at 6.
[248] *Id*.
[249] "The National DNA Data Bank of Canada", Annual Report 2006/2007, [hereinafter "RCMP Annual Report"] at 29.
[250] Reporting Achievement, *supra* note 71 at 4.
[251] RCMP Annual Report, *supra* note 249 at 29.

arguably, be based on correlations found between specific secondary offences, and not a broad statement based only on one or two secondary offences.

It has been argued on the other hand that expansion has not been proven to increase efficiency. Despite the addition of 661,433 DNA profiles to the National DNA database in the United Kingdom in 2006/2007, and in contrast to the figures released by the Home Office (cite 2005 report DNA Expansion), it has also been reported elsewhere that the number of crimes solved only rose by 839.[252] Against expansion, Simoncelli points out that increasing the number of hits (or "matches") does not necessarily mean success of the database, as not all hits will lead to a conviction and must be measured against the "social and financial costs".[253] Writing about the United States, but the argument applies equally elsewhere, she notes that, "the number of hits will not increase proportionately with the number of persons entered into the database. This is because the vast majority of crimes in the United States are committed against property, not persons and […]DNA is often not left or found at the scene of a property crime.[254] Further, she notes that in any case, "DNA found at property crime scenes may not be of sufficient quality and quantity for testing."[255] It has also been argued that even if such crime scenes did have DNA

> local law enforcement hardly has the necessary resources to treat these offences as though they deserved the intensive crime scene effort that is usually reserved for serious violent crimes against the person. In this regard, we noted that it is often difficult enough to convince the police to dust for fingerprints at a residential burglary, because the police know that their search will likely be futile. Imagine, therefore, trying to convince police to search the crime scene (usually outside) of a robbery for such evidence as the perpetrator's hair, tissue, or other residual evidence.[256]

Regarding longer and broader retention periods, including retention of profiles or samples related to those never convicted, it therefore is not certain that there is an efficiency

[252] *Supra* note 231.
[253] *Supra* note 34 at 6.
[254] *Id.* See also Tracy, *supra* note 55 at 686.
[255] *Supra* note 34 at 6.
[256] Tracy, *supra* note 254 at 687.

argument for simply expanding without justifying why certain types of crimes make sense to add to the Databank.

The retention of DNA samples and profiles of those who have not been convicted of a crime has provoked much opposition. Simoncelli says that "subjecting those who have never been convicted of a crime [to being on the forensic DNA databank] subverts our notion of a free and autonomous society and is characteristic of an authoritarian regime."[257] The Human Genetics Commission has also recommended the deletion of innocent people from the National DNA Database in the United Kingdom.[258]

4.2.2 Comments and Recommendations

In summary, there does not appear to be conclusive evidence that a larger DNA databank will necessarily result in a significantly higher rate of convictions. The Privacy Commissioner of Canada has stated, approving the sentiment of the Supreme Court of Canada, that "effectiveness alone cannot provide sufficient justification for unfettered invasion of individual rights. In order for us to feel safer from crime, we must first and foremost have continuing confidence in the reputation and integrity of our criminal justice system which includes respect of individual rights."[259] This type of argument suggests that even if some increase in conviction rates is demonstrated, it must be viewed in relation to the risks associated with the retention of DNA samples and DNA profiles. These risks, amongst others, must be considered in light of any benefits to the criminal justice cause in respect of an expansion in the criminal justice context. At this point, the risks discussed below arguably outweigh any perceived benefits to criminal justice, especially when the evidence does not show significant benefits which may be argued to outweigh the (even hypothetical) risks.

[257] Simoncelli, *supra* note 34 at 2.
[258] *Supra* note 141.
[259] *Supra*, note 221, referring to *R. v. Burlingham* [1995] 2 S. C. R. 206, per Iacobucci J. at para 50, cited with approval by Cory J. in *R. v. Stillman*, [1997] 1 S.C.R. 607, at 126.

This is of course, based on considerations of the weight given to an increase in criminal justice effectiveness versus a decrease in the prioritization of data protection and privacy.

4.3 Risks of Retention

Having established which individuals will be in the DNA databank, the next step is to evaluate what the risks of retaining DNA profiles and DNA samples are. Despite the risks to data protection of DNA samples and DNA profiles retained by law enforcement purposes, including those discussed above, there are also compelling reasons for retaining them. For example, the Federal Bureau of Investigations (FBI) argues that destroying DNA samples and only retaining DNA profiles would "make it impossible to regenerate the database if it were corrupted in some way" or to "introduce new, more sophisticated analytical technologies that would require a re-typing of the original sample; and perform necessary quality assurance checks."[260] Additionally, there is the possibility of using retained samples for re-testing and re-trials leading to exonerations of the wrongfully convicted or conviction of the real perpetrators, as discussed above. Lord Steyn, in the appeal in Marper, even went to so far as saying that "[t]he retention and use of fingerprints and samples [in a DNA databank for the purpose of future matching] does not affect the appellants unless they are implicated in a future crime, by a DNA sample found at the scene."[261]

On the other hand, and in particularly in response to Lord Steyn's comments, there are arguments to be made regarding other potential uses to which collected DNA samples or their profiles could be put. Drilling down further raises questions of the value and risks of retaining both DNA samples and DNA profiles.

[260] Nuffield Report, *supra* note 3 at s. 4.44.
[261] Regina v. Chief Constable of South Yorkshire Police (Respondent) ex parte LS (by his mother and litigation friend JB) (FC) (Appellant) [2004] UKHL 39 at para. 37.

4.3.1 The Risk of Additional Information Being Derived from DNA in a Databank

As has already been discussed above, there is more potential for the derivation of additional information, and uses, from DNA samples than from DNA profiles. Michael Smith recognizes this difference when saying in reference to DNA profiles held by the state, "my privacy would not be noticeably compromised by the state's possession of data about the molecular sequences at thirteen "non-coding" loci on my genome--data that reveals nothing about me except that I am me."[262] For this reason, he claims that "[t]he solution to the privacy problem is to destroy the tissue samples in which individuals' DNA resides"[263] and keep the DNA profiles, which do not tell any more than that individuals match or do not.

While a DNA *profile* may not contain information beyond that used to match a known individual to a crime scene sample, the DNA *sample* itself has, as discussed above, the potential for other personal information to be drawn from it at a later point in time. The retention of DNA samples, as opposed to only DNA profiles, therefore can result in an increased risk of misuse by the mere fact that it continues to be within the control of a government or private lab, and also leaves it subject to future developments that would permit the use of that small size of sample to derive information currently not possible to derive from a DNA, or at least to take from such a small DNA sample.

The Supreme Court of Canada has noted the effect of an order to take DNA from an individual pursuant to the Criminal Code on an individual's "informational privacy interests", stating that DNA contains the "highest level of personal and private information." The Court noted that in a free and democratic society, individuals would wish to maintain and control the dissemination to the state of this "biographical core" and "without constraints on the type

[262] Smith, *supra* note 129 at 103.
[263] *Id.* at 104.

of information that can be extracted from bodily substances, the potential intrusiveness of a DNA analysis is virtually infinite."[264]

The concern related to future, unknown, uses that may be made of DNA was clearly outlined by Ray J. in the Ontario Court of Justice's decision *R. v. T.T.* In refusing to authorize the collection of a DNA sample from a youth convicted of robbery, Ray J. noted that "[t]he assumption behind keeping the biological materials that remain after testing is that new and better testing methods will be found in the future, and the sample can be retested."[265] He pointed out that although presently, the policy is to not test for secondary information such as a predispositions to certain diseases, "the fact is that biological material is retained and kept for future testing according to future policies, which may change from the current ones."[266]

Concerns about the potential risks posed by not destroying DNA samples and keeping only the profiles, however, must be balanced against the potential advantages to the criminal investigation process of keeping the samples. One reason is that future changes in technology may permit the analysis of a DNA sample in a better or more accurate manner. This can both lead to the eventual identification of suspects of unsolved crimes or exoneration of those wrongfully convicted.[267]

The other potential use of new technological or scientific developments is that they may develop techniques for extraction of information beyond that needed for the forensic context, such as the extraction of information about the individual that goes beyond that needed for investigative or evidential purposes. The flip side of this is the use of the same technologies to extract information which could be used in the investigative or evidential

[264] *R. v. R.C.,* [2005] 3 S.C.R. 99, 2005 SCC 61 at para. 28.
[265] *R. v. T.T., supra* note 191 at para. 31.
[266] *Id.* at para. 32.
[267] As of February 11, 2008, the Innocence Project, a nonprofit organization in the United States had successfully overturned 212 wrongful convictions, some of which were based on DNA evidence. See also Truscott (Re), 2007 ONCA 575, available at: http://www.ontariocourts.on.ca/decisions/2007/august/2007ONCA0575.htm.

context, but go further than simply identifying whether there is a match or not, and actually identify unique characteristics about an individual.

Sir Alec Jeffreys predicted that links between DNA and diseases would be discovered during research on the human genome. [268] While progress has been made, Gaensslen notes that "technology for using DNA to find out how a person looks, or what diseases or conditions he is likely to have, is not available now. It may not even be possible in the near future. However, the possibilities should be considered before the reality of these technologies is upon us."[269] Commentators on the subject have shown a rational understanding of the difference in sensitivity between types of information that may be derivable from a DNA sample one day. Gaensslen asks "if tech became available to read physical appearance from the sample, why wouldn't crime labs do it?"[270] Even thought Gaensslen acknowledges that the ability to find physical appearance data in DNA is "no worse than a mug shot", he warns that if medical data were extractable from DNA samples, "[t]he information might help locate someone by tracing prescription drugs they are likely to take or clinic visits they may make. Taking the argument even further, it is not inconceivable that DNA technology could reach a stage where one could predict the likely medical or health conditions of parents or siblings of the DNA donor. Should this sort of information be used to locate relatives, who might know or lead to the whereabouts of the subject?"[271] This type of concern is, of course, more relevant in legal regimes which permit familial searching, such as the United Kingdom.

Gender is already identified as a matter of course in the STR testing in the creation of a DNA profile, as discussed above in reference to both Canada and the United Kingdom.

[268] Christine Rosen, *Liberty, Privacy, and DNA Databases,* The New Atlantis, Number 1, Spring 2003, available at http://www.thenewatlantis.com/publications/liberty-privacy-and-dna-databases [hereinafter "Rosen"].
[269] Gaensslen, R.E. "Should biological evidence or DNA be retained by forensic science laboratories after profiling? No, except under narrow legislatively-stipulated conditions. " Journal of Law, Medicine & Ethics. 34.2 (Summer 2006): 375(5) (2008) at 89.
[270] *Id.* at 88.
[271] *Id.* at 93.

While presently very little information is discernible from a DNA profile, there are nonetheless some inferences that can be drawn even from the "non-coding" parts of the DNA, although such testing would be outside of the scope of permitted testing under both national regimes. Ethnic inferences can be drawn from the frequency of repetition of certain specific alleles looked at in the DNA profile, [272] as can the existence of diabetes.[273] With respect to DNA samples, genetic variations are already being discovered that can identify, from a DNA sample, traits such as hair, eye and skin color,[274] age,[275] ancestry,[276] and exposures to toxins.[277] Looking at the original DNA sample, however, progress is being made to determine hair, eye and skin colour from a DNA sample (not DNA profile), as well as exposures to toxins and health related genetic predispositions to certain physical and mental health conditions. While most testing of a DNA sample for such traits requires a larger size of DNA sample than that presently taken for forensic purposes (or typically recovered from a crime scene), it is not inconceivable that in the future, testing will be possible on smaller samples (or by contrast, the law could be changed to take larger samples).

[272] Nuffield Report, *supra* note 3 at s. 2.17. It is noteworthy that a better determination could be made from testing of specific alleles on the DNA sample, rather than only evaluating the DNA profile (id.).
[273] Forensic Science on Trial, *supra* note 92 at para. 85, citing Williams, Johnson and Martin, *Genetic Information & Crime Investigation*, November 2004.
[274] Ossorio, *supra* note 19 at 278, citing The Future of Forensic DNA Testing: Predictions of the Research and Development Working Group, U.S. Department of Justice, National Institute of Justice (2000): at 91; D. L. Faigman, et al., "DNA Typing," in D. L. Faigman, D. H. Kaye, et al., eds., Science in the Law: Forensic Science Issues (St. Paul: West Group, 2002): 664-761; CODIS website, FBI, available at <http:// www.fbi.gov/hq/lab/codis/index1.htm> (last visited March 3, 2006).
[275] *Id.*, citing T. von Zglinicki, et al., "Human Cell Senescence as a DNA Damage Response," Mechanisms of Ageing & Development 126, no. 1 (2005): 111-117; R. Wadhwa, et al., "Imminent Approaches Towards Molecular Interventions in Ageing," Mechanisms of Ageing & Development 126, no. 4 (2005): 481-490; S. E. Artandi and L. D. Attardi, "Pathways Connecting Telomeres and P53 in Senescence, Apoptosis, and Cancer," Biochemical & Biophysical Research Communications 331, no. 3 (2000): 881-890.
[276] *Id.*, citing M. Bamshad, et al., "Deconstructing the Relationship Between Genetics and Race," Nature Reviews Genetics 5 (2004): 598-608; R. A. Kittles and K. M. Weiss, "Race, Ancestry, and Genes: Implications for Defining Disease Risk," Annual Review of Genomics and Human Genetics 4 (2003): 33-67; V. L. Bonham, E. Warshauer-Baker and F. S. Collins, "Race and Ethnicity in the Genome Era: The Complexity of the Constructs," American Psychologist 60, no. 1 (2005): 9-15.
[277] *Id.*, citing P. W. Brandt-Rauf and S. I. Brandt-Rauf, "Biomarkers -- Scientific Advances and Societal Implications," in M. A. Rothstein, ed., Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era (New Haven, London: Yale University Press, 1997): at 511; R. Jaenisch and A. Bird, "Epigenetic Regulation of Gene Expression: How the Genome Integrates Intrinsic and Environmental Signals," Nature Genetics Supplement 33 (2003): 245-254; L. E. Knudsen, et al., "Genotoxic Damage in Mine Workers Exposed to Diesel Exhaust, and the Effects of Glutathione Transeferase Genotypes," Mutation Research 583 (2005): 120-132; D. Sul, et al., "DNA Damage in Lymphocytes of Benzene Exposed Workers Correlates with Trans, Trans-Muconic Acids and Breath Benzene Levels," Mutation Research 582 (2005): 61-70.

As discussed above in the context of familial searching, the similarity of genetic information between family members can be used to help identify a person's sibling or family.[278] Genetic information can also identify some disease susceptibilities,[279] and recently there have also been predictive tests developed for behavioural characteristics, including susceptibility to develop mental disorders,[280] start smoking, commit arson and other criminal behaviors[281] and addictions of all types, which have been associated with particular genetic markers.[282] Ossorio warns that if genetic testing for specific traits such as physical features, including the identification of genetic markers not yet thought possible, improves the efficiency of investigations or prosecutions, "the pressures for its routine use will be enormous"[283] and that "[o]nce law enforcement personnel begin testing for information beyond the thirteen-STR profile, they have incentives to search a source's genome for a wide variety of sensitive information."[284]

The risks associated with the possibility of future technological advances in this field are, by their nature, hypothetical at this point, but are becoming more real possibilities over time. The risks related to such information being derivable from DNA samples will be mitigated by the legal regime regulating such uses. At present, both Canada and the United

[278] See *supra* at 3.2.
[279] *Id.*, citing Online Mendelian Inheritance in Man, OMIM, McKusick-Nathans Institute for Genetic Medicine, Johns Hopkins University (Baltimore, MD) and National Center for Biotechnology Information, National Library of Medicine (Bethesda, MD), available at <http://www.ncbi.nlm.nih.gov/omim/> (last visited March 3, 2006).
[280] *Id.* at 286 citing See, e.g., News and Editorial Staff of Science, "Discoveries of the Year: The Runners Up: Decoding Mental Illness," Science 302 (2003): 2039; C. P. Jacob, et al., "Cluster B Personality Disorders are Associated with Allelic Variation of Monamine Oxidase A Activity," Neuropsychopharmacology 30 (2005): 1711-1718; Y. Yu, et al., "Association Study of a Functional MAOA-UVNTR Gene Polymorphism and Personality Traits in Chinese Young Females," Neuropsychobiology 52 (2005): 118-121; A. Sawa and S. H. Snyder, "Schizophrenia: Diverse Approaches to a Complex Disease," Science 296 (2002): 692-695.
[281] *Id.*, citing M. A. Rothstein, "Applications of Behavioural Genetics: Outpacing the Science?" Nature Reviews Genetics 6 (2005): 793-798, at 794; C. P. Jacob, et al., "Cluster B Personality Disorders are Associated with Allelic Variation of Monamine Oxidase A Activity," Neuropsychopharmacology 30 (2005): 1711-1718; Y. Yu, et al., "Association Study of a Functional MAOA-UVNTR Gene Polymorphism and Personality Traits in Chinese Young Females," Neuropsychobiology 52 (2005).
[282] *Id.* citing Rothstein, *supra* note 18, at 794; R. C. Hogg and D. Bertrand, "What Genes Tell us about Nicotine Addiction," Science 306 (2004): 983-984; M. N. Potenza, et al., "Shared Genetic Contributions to Pathological Gambling and Major Depression in Men," Archives of General Psychiatry 62 (2005): 1015-1021.
[283] Ossorio, *id.* at 284.
[284] *Id.* at 286.

Kingdom's legal frameworks do not permit the testing of a DNA sample for purposes other than the creation of a DNA profile (consisting of non-coding DNA only). The extent of the risk, therefore, comes from either such testing being done illegally, or a change in the law expanding permitted uses of the DNA sample.

4.3.2 The Risk of "Function Creep"

The phenomenon of "function creep" has been described as "when a project or mission is expanded beyond its original goals, in the case of forensic bioinformation databases, this could be seen by the expansion of databases to include constituencies that were not originally intended as targets, and by extending the uses to which the databases can be put."[285] This paper has examined this issue above in respect of expanding the threshold of offences for inclusion in the DNA databank. The other type of potential expansion, however, is the expansion to permit DNA collected for specific purposes to be legally used for additional purposes.

This could occur in respect of the use of forensic DNA samples for secondary purposes beyond the legislative restriction in the United Kingdom that DNA samples may only be used for "purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution".[286] This is already seen in other contexts. Stories abound in the United States of patients who had their DNA tested by private companies to inform themselves as to their risks of certain diseases, such as breast cancer. They later discovered that the results of such testing was shared with their insurers, resulting in either a denial of coverage or massive increases in rates.[287] This concerns reflect how despite current assurances as to the separation of uses and protection of DNA data, these assurances can

[285] Nuffield Report, *supra* note 3 at 6.19; see also Tracy, *supra* note 55 at 673.
[286] See *supra* note 171.
[287] See e.g. Rosen, *supra* note 268.

disappear as quickly as the law can be changed. A newspaper article[288] reported that in the United Kingdom's military, personnel were asked to submit DNA for identification purposes in the event that they are killed in the line of duty. They submitted DNA with the understanding that it would be kept separate from the National DNA Database. The article about this story expressed concern that:

> If the MoD sticks to the regime it has outlined, there would seem to be few risks to the individuals concerned. However, in a UK which has lately seen sweeping changes based on isolated incidents, there would still seem grounds for concern. It might take no more than a single, well-publicised murder or rape which could have been solved/prevented if only the Forces' DNA samples had been added to the police database, and bingo - the rules of the game could change retrospectively.[289]

Legal changes permitting expanded uses of DNA samples collected for one purpose can also come as a result of a regime change in a country. Since the uses to which such information is used is part of the policy supported by the government of the day, part of the risk of retaining DNA samples beyond the time period required for their forensic use, including DNA samples of persons investigated but ultimately acquitted, is that the over time personal information which was not considered something to hide can become so based on change in circumstances.[290] This is illustrated in the clearly extreme example of the Netherlands, where each citizen's religion was noted as part of state record-keeping for innocuous administrative purposes. However, once the Nazis had access to these records, the availability of this information is thought to have facilitated the killing of Dutch Jews, which was carried out at a rate higher than in any other country.[291]

[288] Lewis Page, "MoD asks UK forces personnel to submit DNA sample, January 28, 2008, available at: http://www.theregister.co.uk/2008/01/28/uk_servicemen_dna_sampling_scheme/.
[289] *Id.*
[290] David Lazer and Viktor Mayer- Schönberge, *Statutory Frameworks For Regulating Information Flows: Drawing Lessons For The Dna Data Banks From Other Government Data Systems*, 34 J.L. Med. & Ethics 366 [hereinafter "Lazer"] at 367, citing S. Cole, *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*, in D. Lazer, ed., *DNA and the Criminal Justice System*: The Technology of Justice (Cambridge, MA: MIT Press, 2004): 63- 90.
[291] Lazer, *id* at 368 W. Seltzer and M. Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses*, Social Research 68 (2001): 481-513.

The issue of the contextual sensitivity of genetic information, in particular once coded, is also discussed by Lazer who notes that that "bits do not wear out with use and may become more potent over time. Genetic information is an extreme example, where data that are not interpretable today might yield great insights tomorrow."[292] This can also be seen in the medical context. As discussed above, there is great possibility that in the future it will be possible to derive sensitive medial data from DNA samples, if not DNA profiles. Simoncelli notes that it is not inconceivable that one day there would be potential for discriminatory treatment in the medical, insurance or education context of those carrying or susceptible to a certain disease or other genetic characteristic. Examples from the recent history of the United States are pointed out by Simoncelli, reminding that "[w]e need only look to the history of our own country, where a eugenics movement resulted in thousands of involuntary sterilizations of the so-called "feebleminded," "abnormal," or "mentally deficient,"[293]

Familial searches are another example of an expanding use of DNA databank data. This expands the information gathered from a DNA databank from searching and matching to start bringing additional individuals into the system and testing presumptions about relations. In terms of data protection, one concern is that familial searching runs the risk of revealing information about family relations that would otherwise be unknown.[294] For example, the collection of DNA from an individual's child, could reveal that the individual is not, in fact, related by blood to his child.[295] Likewise the same scenario could apply with respect to a parent or sibling, where one party does not know that they are not related by blood. For this reason, it is vital that police treat any information such as this with in total confidence.

As well, "[t]here is also the question of whether the use of an individual's databased DNA in this way violates existing promises of privacy and confidentiality made when genetic

[292] *Id*. at 367.
[293] Simoncelli, *supra* note 34 at 5.
[294] Nuffield Report, *supra* note 3 at para. 6.8.
[295] Id.

material was originally collected. Furthermore, the implicit assumptions made about criminality and relatedness may also be problematic."[296] Some comfort is found in the fact that it would, be illegal for police to reveal paternity information, since it is not a purpose set out in the *Police and Criminal Evidence Act, 1984*.[297]

4.3.3 The Risks of Mistakes or Malfeasance

Another risk to data protection comes from the fact of human intervention. Data breaches related to a forensic DNA databank scheme can result equally from a genuine mistake or deliberate malfeasance. These are the types of events that laws may try to account for, but any gaps in legal and operational procedures are subject to error or manipulation. While a legal regime may provide for retroactive punishment of those involved, the harm done by a data breach can be immediate and irreversible. The larger a forensic DNA databank is, in terms of breadth and in terms of whether DNA samples are retained along with DNA profiles, samples being of more risk if disclosed, as discussed above, the greater the number of people potentially exposed to these types of events.

In the past few years, the United Kingdom has experienced a series of high profile embarrassing data losses at the hands of public servants and otherwise. In one extreme example, in October, 2007, discs containing the entire UK child benefit database went missing in transit. The database included passport and national insurance numbers as well as bank details for over 25 million people.[298] The reward offered of £20,000 paled in comparison to the alleged £1.5 billion value to criminals dealing in identity fraud.[299]

[296] Forensic Science on Trial, *supra* note 92 at para. 84.
[297] Nuffield Report, *supra* note 3 at s. 6.9.
[298] "Police Search Tips in Disc Hunt", BBC Online, , December 1, 2007, available at: http://news.bbc.co.uk/2/hi/uk_news/7122401.stm; "MoD to be Quizzed Over Lost Data" BBC online, January 19, 2008, available at: http://news.bbc.co.uk/2/hi/uk_news/7197628.stm.
[299] "Discs worth 1.5bn to Criminals", BBC online, November 28, 2007, available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7117291.stm; "20,000 reward offered for discs", BBC online, December 5, 2007, available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7128851.stm.

With respect to the National DNA Database, in January, 2007, the Netherlands sent a disc containing over 2000 DNA profiles to the United Kingdom to match against the Database. The disc wound up sitting on a desk for over a year until it was checked against the Database in February, 2008. At that time, 15 matches were found, and 11 of those individuals were said to have committed other crimes, some violent, in the UK during that year in which the disc was not checked.[300] While the ultimate effectiveness of the search once finally conducted shows that matches were found, the delay and errors in the process were described in the press as "just the latest example of government's failure to follow even simple procedures when dealing with sensitive information."[301] Regarding the Ministry of Defense collecting DNA from service personnel, following his comments regarding the possibility of function creep following policy change, the journalist quoted above added, "Then, of course, there's the chance that the MoD will simply manage to lose all its files or let them be stolen/copied/mixed up - not unlikely, given the recent record of the British government in this area."[302]

While the Council Decision procedures for direct access will mean that there will be fewer instances of DNA profiles on portable media such as discs being shared between government agencies, the United Kingdom has had such a high rate of data losses and breaches that the ability to protect this type of data must be considered. Further concerns related to mistakes made in respect of the DNA Database is a 2008 report that there were said to be over 550,000 false, miss-spelt or incorrect names on the UK DNA database, which is 1 in 8 entries.[303]

[300] "DNA Disc Failings 'Catastrophic'", BBC Online, January 20, 2008, available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7253989.stm.
[301] John Oates, "Government 'lost' DNA data on 2,000 criminal suspects" The Register, February 20, 2008, available at: http://www.theregister.co.uk/2008/02/20/government_data_loss/.
[302] *Supra* note 288.
[303] Whereisyourdata.co.uk, "DNA Errors", July 3, 2008, available at: http://www.whereisyourdata.co.uk/whereismydata/2008/07/03/dna-errors/.

It is noteworthy that in a telephone call with a Senior Policy Analyst from the Office of the Privacy Commissioner, he noted that the Commissioner's office has never questioned the management and security of the Data Bank with respect to controls, restrictions or use of information once it is in the Data Bank. Rather, the Office's concern is in respect of expansion, including if that expansion is through adding new offences, permitting familial searches, volunteer samples, or whether through permitting DNA sample to be taken earlier in the criminal process, as is done in the United Kingdom.[304] In a call with the National DNA Data Bank in Canada it was confirmed that Canada has not experienced any data breaches or losses of the kind seen in the United Kingdom.[305]

The risk of loss or breach expands, however, as function creep expands the permitted uses and sharing of such data. To the extent that more direct access is given to the databank, the higher the risk of someone finding a way around security measures. Likewise, a larger databank may require different technology and, possibly, more individuals with access to it. Each of these can increase the risk of an accident or a rogue employee taking advantage of a security flaw.

In addition to the threats to an individual's informational privacy as discussed in Chapter 1,[306] it has been argued that simply being part of such a databank can have implications based on being brought into a criminal investigation, including the distress and stigma attached to the process, even if one is innocent.[307] For example, there may also be perceived a presumption of criminality by mere inclusion in such a forensic databank.[308] It has therefore been argued that "it is not irrational for a person to object to the retention of

[304] OPC Interview, *supra* note 20.
[305] DNNB Interview, *supra* note 123.
[306] See *supra* at s. 1.6.
[307] *Id*.
[308] Nuffield Report, *supra* note 3 at s. 3.25.

their biological sample and DNA profile on the Database if they have never committed a criminal act in their whole life nor will ever do so."[309]

Further, any data or security breach would affect more people simply because more people are in the database. Without differentiation in treatment being made based on the applicable offence or outcome of investigation, someone who was simply investigated, but ultimately acquitted, in respect of bicycle theft would be affected by any risk or breach of data protection in the same manner as someone who has been convicted of murder, as each are equally exposed to the risk by their common presence in the forensic DNA database. While neither may "deserve" to have their bioinformation, used for secondary purposes, accessed illegally or otherwise tampered with, it is even more difficult to justify why someone without *any* criminal past should be in the same shoes as hardened criminals with respect to any risks related to their DNA being stored in a DNA databank.

4.4 Recommendations

Having reviewed the legislative frameworks for forensic DNA databank regimes in Canada and the United Kingdom, this paper will now propose some general recommendations as to how the data protection risks discussed above can be best handled through legal structures. The first step, as discussed above, is to ensure that no more people are on the national DNA databank than need be. As was demonstrated with the examples of Canada and the United Kingdom, where that line "need be", however, is a matter of policy and differs by country. To the extent that an increase in DNA databank size has not been demonstrated to conclusively produce significant returns, the line should be drawn closer to the end of excluding, rather than including, people in the databank by default. This means taking an approach closer to that of Canada, and not retaining DNA samples or profiles of persons other than those convicted. Further, the list of offences in respect of which the DNA

[309] *Id*.

databank regime applies should be limited to: (i) only offences for which DNA evidence would be of investigative or evidential value; and (ii) only the most serious offences.

Regarding what considerations should be taken into account when a legal regime is determining which offences should carry with them the right for police to take a DNA sample, this paper will use bicycle theft as an example. Although bicycle theft could be a crime solvable with DNA evidence, it could also be solved with fingerprints. Whereas in the United Kingdom DNA may be taken in respect of bicycle theft, in Canada it may not. Fingerprints on record with the police, providing less personal information to the government than a DNA sample, can still be compared to prints found on the bicycle. Therefore the crime of bicycle theft could be handled with fingerprints and need not be an offence in respect of which DNA samples may be taken. Short of a link demonstrating that bicycle thieves are likely to grow up to become violent criminals,[310] the argument that it is better to take a DNA sample now in order to have it on record going forward fails to justify the taking of more sensitive personal information (DNA) than is necessary (fingerprints).

Having limited the number of people whose DNA is collected in the criminal context, it is equally important to have appropriate legal measures in place to regulate the use made of the retained DNA profiles and samples. As both Canada and the United Kingdom have, laws should explicitly limit the uses that can be made of DNA samples and profiles. DNA samples should only be permitted to be used for the creation of DNA profiles using the national standard for non-coding markers, but nothing else. With respect to the DNA profile, similarly, it should only be permitted to be used for forensic purposes.

Retention of DNA samples and DNA profiles raises harder questions. As discussed above, since DNA profiles are less of a risk in respect of secondary uses, their retention

[310] See *supra* at s. 4.1 for arguments from law enforcement agencies linking certain minor crimes to more serious ones. Notably bicycle theft is not given as an example of such a minor crime from the Home Office although it appears on the list of Recordable Offences in respect of which a DNA sample may be taken.

makes sense in terms of both economic and forensic terms. They can be used to populate a DNA databank which will grow as the number of DNA profiles grow.

With respect to DNA samples, there are stronger arguments against their retention, including the risks discussed in this Chapter 4. While having in place legal prohibitions against secondary uses of DNA samples is, technically, one way to control use beyond the original forensic purpose of identification, this paper has addressed the limitations of legal restrictions in the face of changing technology, governments, globalization and criminal justice priorities of the day. The best pre-emptive defense against all of these is to not have the government hold DNA samples in the first place beyond the time needed for evidentiary purposes.

The risks mentioned above must, however, be balanced against the uses that can be made of DNA samples in the criminal justice field such as later re-testing (for identification purposes only) leading to exonerations of the wrongfully convicted or convictions of the actual offender. This would suggest a middle approach. Starting with the assumption that DNA samples would only be retained in respect of those who were actually convicted, and only in respect of the most serious offences for which DNA could have evidential value, one such potential approach would be for the State to retain DNA samples only for the length of time that the individual is incarcerated. Once released, their DNA sample could be destroyed. This would give the opportunity for exoneration, but would not involve retaining DNA samples longer than needed. If the individual were involved in a future crime, his or her DNA profile would still be on the DNA databank for matching purposes.

There are as many variations possible for how a DNA databank system could be arranged as can be conceived, so the possibilities should be carefully considered and a privacy and data protection impact analysis should be conducted as a matter of course. A system should be chosen to maximize data protection in respect of the DNA samples and

DNA profiles held while still permitting retention of DNA information truly required for identification (but *only* identification) purposes. Where lines are drawn with respect to data protection as a matter of necessity reflect the consent of the individuals involved, so governments should prioritize input from citizens who will be affected as to where they believe these lines should be drawn and what information they would be willing to share and for what purposes in order to improve the criminal justice system.

Avoidance of secondary purposes will require that adequate safeguards are also in place, including operational (e.g. oversight, limited access on a need-to-know basis and separation of the DNA profile and sample from identifying information such as a name), technical (e.g. only collect a small enough size of DNA sample that additional tests cannot be done on it, has passwords on computers) and physical (e.g. lock the doors) measures.

Finally, once a national regulation of a DNA databank is in place and is one which protects DNA data as recommended above, international standards for sharing of or access to DNA databank information (which themselves may stifle the kind of creativity encouraged above when meeting such standards) should ensure that they do not expose countries with stringent data protections to weaker protections of other countries. National laws should require that a country receiving DNA data enter into agreements with the supplying country to ensure the protection of that data, including that it not be used for any secondary purposes, appropriate security measures be put in place while the data is in the receiving country's custody and destruction of the data once it is no longer needed for that forensic purpose.

CONCLUSION

The existence, use and expansion of DNA databanks is a very relevant issue today, including in light of international anti-terrorism concerns. Despite the evidentiary advantages that DNA evidence brings to the criminal justice realm, its collection and retention also raises the possibility of issues related to secondary uses and disclosures which go beyond what is forensically necessity. Having reviewed and compared the legal frameworks regulating DNA databanks in Canada and the United Kingdom above with respect to their approaches to data protection issues and made recommendations as to best practices, the following conclusions may be drawn from the research undertaken here.

There is enormous pressure coming from both those in favour of and those against expansion of national DNA databanks, pitting increased effectiveness in the criminal justice system against the erosion of privacy principles and the increased risk of abuses of data protection. Laws regulating DNA databanks should be forward-looking enough to contemplate the potential for technological, legal and governmental changes and create a DNA databank regime in which data protection and criminal justice interests can both be respected and one need not be strengthened only at the other's expense. Certain aspects of such a system were set out above as recommendations flowing from the sample countries reviewed in this paper.

Having carried out the research and proposed the recommendations above based on that research, this paper concludes that in general the forensic DNA databank system in Canada respects data protection to a greater extent than in the United Kingdom. As well, it is better prepared in the events of changes in technology resulting in potentially expanded uses of DNA information. In summary, as was illustrated in greater detail in the research above, the following indicators support such a claim:

(i) With respect to transparency, Canada's DNA databank regime is more clearly articulated in law and more accessible by individuals as it is set out in a comprehensive manner in a limited number of pieces of legislation, whereas the United Kingdom's system is governed by an array of legislation, amendments and in some cases left unregulated, making information about the DNA databank regime less transparent and more difficult to be accessed by the public;

(ii) With respect to collection of DNA samples, Canadian law sets a significantly higher threshold for collection than the United Kingdom regime does, tying collection to only the most serious offences. The United Kingdom on the other hand, has an expansive list of offenses in respect of which a DNA sample may be collected, including many relatively minor, non-violent, offences. As well, Canadian law requires judicial oversight before a DNA sample may be taken for investigative purposes or be included in the National DNA Data Bank, a step which the United Kingdom's regime does not include, and which further limits the inclusion of individuals in the national DNA databank system.

(iii) With respect to retention, Canada retains a significantly smaller number of DNA samples and DNA profiles than the United Kingdom does. Most notably, whereas Canadian law requires the destruction of DNA samples and profiles if the individual is not convicted, the United Kingdom permits their retention. This, in combination with the lower threshold for collection discussed above, results in a much larger DNA databank in the United Kingdom than in Canada (or anywhere else, for that matter). As was demonstrated in this paper, simply being in the DNA databank exposes an

individual's sensitive personal information to risks related to use and disclosure, to which it would not be otherwise exposed.

(iv) With respect to treatment of volunteers, Canada does not include volunteer DNA samples in the DNA databank as there is no provision for their inclusion in Canadian law. United Kingdom's DNA databank, on the other hand, offers volunteers the option to be included, that choice however is irrevocable.

(v) With respect to the treatment of victims vs. that of offenders, Canada's retention procedures keep victims' DNA samples and profiles out of the Convicted Offenders Index, as there is no provision for their inclusion, rather they are housed in the Crime Scene Index database. In the United Kingdom, by contrast, victims, volunteers, offenders and those arrested but found innocent, are all on one single database.

(vi) With respect to protecting DNA housed in forensic DNA databanks from secondary uses, both Canada and the United Kingdom have laws in place limiting uses of DNA samples and profiles to only specific forensic purposes.

(vii) With respect to familial searches, Canada's system does not permit such use of DNA, whereas the United Kingdom does permit it, by special authorization.

(viii) With respect to sharing data internationally, the two regimes appear equivalent. Canada's laws require that contractual protections be in place with the other country, but no specific requirements are enumerated. Through the Council Decision, the United Kingdom's DNA databank is now subject to access by other EU member States. Having the DNA databank with the greatest number of individuals on it in the European Union, the United Kingdom's participation in international cooperation such as the Council Decision equally makes more people's data available to the other European

Union members. While this may be advantageous from a criminal justice perspective, it exposes more people's sensitive personal data to a wider range of persons and legal regimes. The failure to fully account for the lack of harmonization of DNA databank regimes was one criticism of EU Data Protection Supervisor discussed above.[311]

(ix) With respect to expansion of the databank, the United Kingdom has expanded further than any other DNA databank in the world, however as discussed above, Canada's laws have been moving in the direction of expansion and law enforcement agencies would like to see it continue to do so.

(xi) With respect to human error or malfeasance, both countries' systems naturally have risks of this occurring, however the United Kingdom's government has shown a troubling pattern of data handling mistakes resulting in massive data losses and thefts which raises concern about whether similar risks exist for data held in its DNA databank.

Based on the above summary of comparisons of the research described in more detail above in this paper, it is concluded that Canada's system better protects data of individuals held in its national DNA databank than the United Kingdom. Further, from the research set out above, recommendations were made in Section 4.4 of this paper, above, based on approaches found to be taken by each country. Canada's system more closely matches the recommended approach.

DNA databanks have proven themselves to be a wonderful tool in solving crimes and the data protection risks discussed above need not slow down the progress that DNA evidence has brought to criminal investigations and prosecutions. This paper has demonstrated the significance of ensuring that a national DNA databank regime is conceived

[311] See, *supra*, at 3.3.2.

with data protection concerns in mind. The implications of anything less than such a legal framework can expose individuals' most sensitive personal data – their genetic composition – to unnecessary risks. Acknowledging that many of the risks discussed above are hypothetical to the extent that they would only apply in the event of technological and scientific advances, it is all the more important to address these issues now through appropriate legal frameworks so that once such technology becomes a reality, the laws are in place as needed to ensure that such advancements are not abused.

BIBLIOGRAPHY

Statutory Materials

Canada

An Act to amend certain Acts in relation to DNA identification, 2007, c.22;

An Act to amend the Criminal Code, the DNA Identification Act and the National Defence Act, S.C. 2005, c.25.

Anti-Terrorism Act, 2001, c. 41.

Criminal Code, R.S., 1985, c. c.46.

DNA Identification Act, R.S., 1998, c. 37.

Privacy Act, R.S. 1985, c. P-21.

Youth Criminal Justice Act, 2002, c.1.

United Kingdom

Criminal Justice Act, 2003, c. 44.

Criminal Justice and Police Act, 2001, c. 16.

Criminal Justice and Public Order Act, 1994, c. 33.

Data Protection Act, 1998, c. 29.

National Police Records (Recordable Offences) Regulations 2000, S.I. 2000/1139, as amended.

Schedule to the Recordable Offences Regulations 2000.

Police and Criminal Evidence Act, 1984, c. 60.

International Instruments

Recommendation R (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system (1992).

Recommendation No. R (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies).

Explanatory Memorandum to Recommendation No. R (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system, (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the ministers' deputies).

Council Decision on the Stepping up of Cross-Border Cooperation, Particularly in Combating Terrorism and Cross-Border Crime, 11896/07, Council of the European Union, Brussels 17 September 2007.

Treaty on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, Brussels, 7 July 2005 (28.07).

Case Law

Canada

R. v. Burlingham [1995] 2 S. C. R. 206, per Iacobucci J. at para 50, cited with approval by Cory J. in *R. v. Stillman*, [1997] 1 S.C.R. 607.

R. v. Harris. [2008] O.J. No. 1976, Ontario Superior Court of Justice, D.M. Brown J., May 16, 2008.

R. v. R.C., [2005] 3 S.C.R. 99, 2005 SCC 61.

R v. S.A.B. [2003] 2 S.C.R. 678.

R. v. T.T. [2001] O.J. No. 2936.

United Kingdom

Regina v. Chief Constable of South Yorkshire Police (Respondent) ex parte LS (by his mother and litigation friend JB) (FC) (Appellant) and Regina v. Chief Constable of South Yorkshire Police (Respondent) ex parte Marper (FC) (Appellant) (consolidated appeals) [2004] UKHL 39.

Regina v. Chief Constable of South Yorkshire Police (Respondent) ex parte LS (by his mother and litigation friend JB) (FC) (Appellant) [2004] UKHL 39.

European Court of Human Rights

S. & Michael Marper v. The United Kingdom, Application nos. 30562/04 and 30566/04 Decision on Admissibility.

Articles

Paul Chadwick, *The Value of Privacy*, E.H.R.L.R. 2006, 5, 495 [hereinafter "Chadwick"] at 504-5.

Frederico & Rondinelli's DNA Netletter, March 1, 2008, Issue 98.

Frederico & Rondinelli's DNA Netletter, April 1, 2008 - Issue 99.

Frederico & Rondinelli's DNA Netletter, June 1, 2008, issue 101.

R. E. Gaensslen, *Should biological evidence or DNA be retained by forensic science laboratories after profiling? No, except under narrow legislatively-stipulated conditions,* Journal of Law, Medicine & Ethics. 34.2 (Summer 2006): 375(5) (2008).

Emanuel Gross, *The Struggle Of A Democracy Against Terrorism--Protection Of Human Rights: The Right To Privacy Versus The National Interest--The Proper Balance*, 37 Cornell Int'l L.J. 27.

David Lazer and Viktor Mayer- Schönberge, *Statutory Frameworks For Regulating Information Flows: Drawing Lessons For The DNA Data Banks From Other Government Data Systems,* 34 J.L. Med. & Ethics 366.

Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. Ottawa L. & Tech. J. 357 (2005).

A. Wayne McKay, *Human Rights in the Global Village: The Challenges of Privacy and National Security*, 20 Nat'l J. Const. L. 1 (2006).

Thomas J. Moyer, Chief Justice & Stephen P. Anwa, *Biotechnology and The Bar: A Response To The Growing Divide Between Science And The Legal Environment*, 22 Berkley Tech. L.J. 671 (2006) at 673.

Pilar N. Ossorio, *About Face: Forensic Genetic Testing For Race And Visible Traits*, 34 J.L. Med. & Ethics 277

Rebecca Sasser Peterson, *When Fear Goes Too Far,* 37 Am. Crim. L. Rev. 1219 at 1221, citing J. Clay Smith, *The Precarious Implications of DNA Profiling*, 55 U. PITT. L. REV. 865, 869 (1994).

Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34 J.L. Med &Ethics 153.

Tania Simoncelli, *Dangerous excursions: the case against expanding forensic DNA databases to innocent persons*, Journal of Law, Medicine & Ethics. 34.2 (Summer 2006): 390(8).

Julie A. Singer, Monica K. Miller & Meera Adya, *The Impact of DNA and Other Technology on the Criminal Justice System: Improvements and Complications*, 17 Alb. L.J. Sci. & Tech. 87 (2007).

Michael E. Smith, *Let's make the DNA identification database as inclusive as possible.(DNA Fingerprinting and Civil Liberties),* Journal of Law, Medicine & Ethics. 34.2 (Summer 2006): 385(5) 2008.

Daniel J. Steinbock, *Data Matching, Data Mining, And Due Process*, 40 Ga. L. Rev. 1 at 6-7 (2005).

Paul E. Tracy & Vincent Morgan, *Big Brother and His Science Kit: DNA Databases for 21st Century Crime Control?* 90 J. Crim. L. & Criminology 635, 688-89 (2000).

Internet Resources

Websites

Forensic Science Service: *Casefile "Colin Pitchfork - first murder conviction on DNA evidence also clears the prime suspect"*, available at: http://www.forensic.gov.uk/html/media/case-studies/f-18.html (last visited 10 October, 2008).

Genewatch UK, *A Brief Legal History of the NDNAD*, available at: http://www.genewatch.org/sub-537968.

Genewatch, "Exceptional Case Procedures for Removal DNA, Fingerprints and PNC Records", April 24, 2006, available at: http://www.genewatch.org/sub-539488.

Home Office Forensic Science and Pathology Unit, "DNA Expansion Programme 2000–2005: Reporting Achievement", available at: http://police.homeoffice.gov.uk/publications/operational-policing/DNAExpansion.pdf.

House of Commons Science and Technology Committee, *Forensic Science on Trial*, Seventh Report of Session 2004-2005, available at: http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/9607.htm#a20.

HBO, "The Good Doctor", available at: http://www.hbo.com/autopsy/episode/episode_7_the_good_doctor.html.

Innocence Project, available at: http://innocenceproject.org/.

National DNA Data Bank Update, August 18, 2008, available at: http://www.nddb-bndg.org/stats_e.htm (last updated 12 March, 2008).

National DNA Data Bank, available at: http://www.nddb-bndg.org/main_e.htm (last updated 1 September, 2006).

National DNA Data Bank, *Protecting Privacy*, available at: http://www.nddb-bndg.org/pri_secu_e.htm (last updated 23 April, 2007).

National DNA Data Bank, Annual Report 2006/2007
Forensic Data Center, *Short Tandem Repeats,* available at: http://www.forensicdnacenter.com/dna-str.html (last visited 10 October, 2008).

Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical Issues*, (September, 2007), available at: http://www.nuffieldbioethics.org/go/ourwork/bioinformationuse/introduction.

Parliamentary commentary to Bill C-13. Online at http://www.parl.gc.ca/common/Bills_ls.asp?Parl=38&Ses=1&ls=C13 - 15.

Presentation to the Standing Committee on Justice and Human Rights, Bruce Phillips, (February 12, 1998), available at: http://www.privcom.gc.ca/speech/archive/02_05_a_980212_e.asp.

Privacy Commissioner of Canada, Statement to the Subcommittee on Public Safety Act and National Security, June 1, 2005, available at: http://www.privcom.gc.ca/speech/2005/sp-d_050601_e.asp;

Statistics Canada, Daily Population Estimates, available at: http://www.statcan.ca/Daily/English/080929/d080929b.htm (last visited on 29 September, 2008).

U.S. Department of Energy, Office of Science, Human Genome Project Information, *DNA Forensics,* available at: http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml (last updated 16 September, 2008).

Where is your Data?, "ACPO Guidelines for DNA Retention", available at: http://www.whereisyourdata.co.uk/whereismydata/2008/08/16/acpo-guidelines-for-dna-retention/ (last visited16 August, 2008).

Where is your Data?, "DNA Errors", July 3, 2008, available at: http://www.whereisyourdata.co.uk/whereismydata/2008/07/03/dna-errors/.

Online Newspaper Articles

BBC Online, "Police Search Tips in Disc Hunt", December 1, 2007, available at: http://news.bbc.co.uk/2/hi/uk_news/7122401.stm.

BBC Online, "MoD to be Quizzed Over Lost Data", January 19, 2008, available at: http://news.bbc.co.uk/2/hi/uk_news/7197628.stm.

BBC Online "DNA Disc Failings 'Catastrophic'", February 20, 2008, available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7253989.stm.

Andy Bloxham, "DNA bank solves one crime per 800 profiles", May 6, 2008, available at http://www.telegraph.co.uk/news/uknews/1929849/DNA-bank-solves-one-crime-per-800-profiles.html.

CBCNews.ca, "DNA Samples Invade Privacy, Critics Say", May 23, 2003, available at: http://www.cbc.ca/canada/story/2003/05/23/jone030523.html.

CTV.ca "TO Police Defend Requesting DNA Samples", May 22, 2003, available at: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20030522/hollyjones_investigation_20030522?s_name=Autos&no_ads=.

Christopher Hope "DNA Profiles of one million innocent people should be erased, watchdog says", July 30, 2008, available at: http://www.telegraph.co.uk/news/newstopics/politics/2471425/DNA-profiles-of-one-million-innocent-people-should-be-erased-watchdog-says.html.

Christopher Hope "Profiles of 40,000 innocent children on DNA database", August 15, 2008, available at: http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/2565016/Profiles-of-40000-innocent-children-on-DNA-database.html.

David Mery, "How to Delete Your DNA Profile", 7 January, 2008, available at: http://www.theregister.co.uk/2008/01/07/delete_your_dna_profile/.

Nigel Morris, "A 'chilling' proposal for a universal DNA database", September 6, 2007, available at: http://www.independent.co.uk/news/uk/crime/a-chilling-proposal-for-a-universal-dna-database-401503.html.

Anahad O'Connor, The New York Times, *The Claim: Identical Twins Have Identical DNA*, March 11, 2008, available at: http://www.nytimes.com/2008/03/11/health/11real.html?_r=1& ref=science&oref=slogin.

John Oates, "Government 'Lost' DNA Data on 2,000 Suspects", February 20, 2008, available at: http://www.theregister.co.uk/2008/02/20/government_data_loss/

James Orr, "Judge wants everyone in UK on DNA database", September 5, 2007, available at: http://www.guardian.co.uk/uk/2007/sep/05/humanrights.ukcrime.

OUT-LAW News, "Police will share data across Europe against privacy chief's advice" 14/06/2007, available at: http://www.out-law.com//default.aspx?page=8148.

Lewis Page, "MoD asks UK Forces personnel to submit DNA samples", January 28, 2008, available at: http://www.theregister.co.uk/2008/01/28/uk_servicemen_dna_sampling_scheme/.

Christine Rosen, *Liberty, Privacy, and DNA Databases,* The New Atlantis, Number 1, Spring 2003, available at: http://www.thenewatlantis.com/publications/liberty-privacy-and-dna-databases (last visited 19 November, 2008)

Mark Townsend and Anushka Asthana, The Guardian, "Put young children on DNA list, urge police", March 16, 2008, available at: http://www.guardian.co.uk/society/2008/mar/16/youthjustice.children.

Richard Willing, "CSI Effect' has Juries Wanting More Evidence, USA Today, Aug. 5, 2004, available at: http://www.usatoday.com/news/nation/2004-08-05-csi-effect_x.htm?loc=interstitialskip (last visited 10 October, 2008).

Rick Westhead, "Widen DNA Dragnet: Blair", April 12, 2008, available at: http://www.thestar.com/News/GTA/article/413851.

Interviews

Telephone call with Carman Baggarley, Senior Policy Advisor, Office of the Privacy Commissioner of Canada, telephone call Sept. 3, 2008.

Telephone call with Andre Savoie, acting manager, collection and training, National DNA Data Bank on 12 September, 2008.