2010

The legal, social and ethical controversy of the collection and storage of fingerprint profiles and DNA samples in forensic science

Katina Michael
University of Wollongong

Publication Details

Michael, K. (2010). The legal, social and ethical controversy of the collection and storage of fingerprint profiles and DNA samples in forensic science. In K. Michael (Eds.), 2010 IEEE International Symposium on Technology and Society: Social Implications of Emerging Techologies (pp. 48-60). Singapore: IEEE.

The legal, social and ethical controversy of the collection and storage of fingerprint profiles and DNA samples in forensic science

Abstract
The collection and storage of fingerprint profiles and DNA samples in the field of forensic science for nonviolent crimes is highly controversial. While biometric techniques such as fingerprinting have been used in law enforcement since the early 1900s, DNA presents a more invasive and contentious technique as most sampling is of an intimate nature (e.g. buccal swab). A fingerprint is a pattern residing on the surface of the skin while a DNA sample needs to be extracted in the vast majority of cases (e.g. at times extraction even implying the breaking of the skin). This paper aims to balance the need to collect DNA samples where direct evidence is lacking in violent crimes, versus the systematic collection of DNA from citizens who have committed acts such as petty crimes. The legal, ethical and social issues surrounding the proliferation of DNA collection and storage are explored, with a view to outlining the threats that such a regime may pose to citizens in the not-to-distant future, especially persons belonging to ethnic minority groups.

Disciplines
Physical Sciences and Mathematics

Publication Details
Michael, K. (2010). The legal, social and ethical controversy of the collection and storage of fingerprint profiles and DNA samples in forensic science. In K. Michael (Eds.), 2010 IEEE International Symposium on Technology and Society: Social Implications of Emerging Techologies (pp. 48-60). Singapore: IEEE.

The Legal, Social and Ethical Controversy of the Collection and Storage of Fingerprint Profiles and DNA Samples in Forensic Science

Katina Michael
School of Information Systems and Technology, Faculty of Informatics, University of Wollongong
katina@uow.edu.au

Abstract

The collection and storage of fingerprint profiles and DNA samples in the field of forensic science for non-violent crimes is highly controversial. While biometric techniques such as fingerprinting have been used in law enforcement since the early 1900s, DNA presents a more invasive and contentious technique as most sampling is of an intimate nature (e.g. buccal swab). A fingerprint is a pattern residing on the surface of the skin while a DNA sample needs to be extracted in the vast majority of cases (e.g. at times extraction even implying the breaking of the skin). This paper aims to balance the need to collect DNA samples where direct evidence is lacking in violent crimes, versus the systematic collection of DNA from citizens who have committed acts such as petty crimes. The legal, ethical and social issues surrounding the proliferation of DNA collection and storage are explored, with a view to outlining the threats that such a regime may pose to citizens in the not-to-distant future, especially persons belonging to ethnic minority groups.

1. Introduction

The aim of this paper is to apply the science, technology and society (STS) studies approach which combines history, social study and philosophy of science to the legal history of DNA sampling and profiling in the United Kingdom since the first forensic use of DNA in a criminal court case in 1988. The paper begins by defining the application of biometrics to the field of criminal law, in particular the use of fingerprint and DNA identification techniques. It then presents the differences between fingerprints and DNA evidence and focuses on distinguishing between DNA profiles and samples, and DNA databanks and databases. Finally the paper presents the legal, ethical and social concerns of the proliferation of DNA collection and storage in particular jurisdictions prior to 2010 (e.g. United Kingdom). The paper points to the pressing need for the review of the *Police and Criminal Evidence Act 1984*, and to the procedures for DNA collection and storage in the U.K.'s National DNA Database (NDNAD) which was established in 1995. Some examples are provided of the state of play in the United States as well.

2. Conceptual Framework

It is of no surprise that in recent years there has been a convergence between science and technology studies (STS) and law and society (L&S) studies. Some commentators, like this author believe that there is a need to define a new theoretical framework that amalgamates these increasingly converging areas. Lynch et al. [6, p.14] write: "[w]hen law turns to science or science turns to law, we have the opportunity to examine how these two powerful systems work out their differences." This convergence has its roots planted in legal disputes in the fields of health, safety and environmental regulation. For instance, advances in technology have challenged ones right to live or die. New innovations have the capacity to draw out traditional distinctions of regulations or they can challenge and even evade them.

In this paper we study the "DNA controversy" using the conceptual framework that can be found in Figure 1 which depicts the role of major stakeholders in the debate. In the early 1990s the "DNA Wars" [6] focused on two major problems with respect to the techno-legal accountability of DNA evidence in a court of law. The first had to do with the potential for error in the forensic laboratory, and the second had to do with the combination of genetic and statistical datasets. And it did not just have to do with legal and administrative matters, but issues that were both technical and scientific in nature. The key players included expert lawyers, scientists who actively participated in legal challenges and public policy debates, and the media who investigated and reported the controversy [6]. To put an end to the controversy would require the coming together of law, science and the public in a head-on confrontation. And that is indeed what occurred. By the late 1990s DNA had become an acceptable method of suspect identification and a great number of onlookers prematurely rushed to declare a closure to the controversy although as commentators have stated there was no moment of truth or definitive judgment that put an end to the controversy. What many did not recognize at the time however, is that the DNA

controversy would return, in places like the United Kingdom, bigger and with more intensity than ever before.

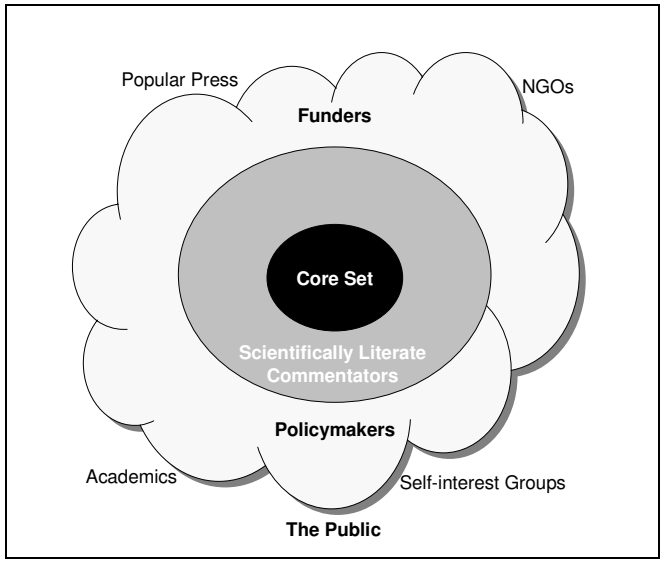


Figure 1. The Core Set Diagram: Studying the DNA Controversy

It is with great interest to read that closure in the DNA controversy was really visible when the NDNAD and some of the legislation and policy surrounding it facilitated talks between nations in Europe with respect to harmonization. According to Lynch et al. [6, p.229]:

> "[e]fforts were made to "harmonize" DNA profile and database standards in Europe, and other international efforts were made to coordinate forensic methods in order to track suspected "mobile" criminals and terrorists across national borders. These international efforts to implement and standardize DNA profiling contributed to closure in particular localities by demonstrating that the technique was widely used and had become a fixture of many criminal justice systems."

While closure it may have signified to those working within an STS and L&S approach, harmonization was certainly not reached. Far from it, the U.K. who had been responsible for initial harmonization efforts, later, lost its way. What made onlookers believe that closure had fully occurred were the technical, legal and administrative fixes that had taken place. But closure in this instance did not mean the complete end to the controversy- no- what was coming was much greater disquiet in the U.K, and this period was named 'post-closure' by the STS and L&S commentators. Postclosure signals a period of time after closure is established, when the possibilities for issues that were once closed are reopened. In the case of the NDNAD in the U.K. it was not old issues that were reopened during postclosure, but new issues that were introduced due to so-called legal fixes. These legal fixes had social implications, so it was not until the public and the media and non-government organizations alongside self-interest groups were satisfied that change would be imminent, that postclosure seemed a real possibility. The threat to the post-closure of the DNA controversy however, is the burgeoning demand for DNA samples in fields such as epidemiology research and the recent commercialization of DNA sample collection and storage for every day citizens (e.g. DNA home kits selling for less than $100US dollars). DNA is no longer seen as just useful for forensic science or health, and this is placing incredible pressure on the advanced identification technique which is increasingly becoming commoditized.

3. Background: What is Biometrics?

As defined by the Association for Biometrics (AFB) a biometric is "...a measurable, unique physical characteristic or personal trait to recognize the identity, or verify the claimed identity, of an enrollee." The physical characteristics that can be used for identification include: facial features, full face and profile, fingerprints, palmprints, footprints, hand geometry, ear (pinna) shape, retinal blood vessels, striation of the iris, surface blood vessels (e.g., in the wrist), and electrocardiac waveforms [1]. Other examples of biometric types include DNA (deoxyribonucleic acid), odor, skin reflectance, thermogram, gait, keystroke, and lip motion. Biometrics have seven characteristics: they are universal in that every person should possess that given characteristic; they are unique in that no two persons should have the same pattern; they are permanent in that they do not change over time; they are collectable and quantifiable; there is performance in that the measure is accurate, it is acceptable to users; and circumventing, meaning that the system of identification theoretically cannot be duped [2]. The two most popular methods of identification today in criminal law, when direct evidence is lacking such as a first hand eyewitness account, are fingerprinting and DNA.

4. What is Fingerprinting?

Fingerprints are classified upon a number of fingerprint characteristics or unique pattern types, which include arches, loops and whorls [3, p.228]. If one inspects the epidermis layer of the fingertips closely, one can see that it is made up of ridge and valley structures forming a unique geometric pattern. The ridge endings are given a special name called minutiae. Identifying an individual using the relative position of minutiae and the number of ridges between minutiae is the traditional algorithm used to compare pattern matches. As

fingerprints do not change from birth until death unless they are accidentally or deliberately deformed, it is argued that they can provide an absolute proof of identity. The science of fingerprint identification is called *dactyloscopy* [4, p.4].

4.1. Fingerprinting as Applied to Criminal Law

Fingerprints left behind at the scene of a crime (SOC) can be used to collect physical evidence for the purposes of human identification. They have the capacity to link a person (e.g. a suspect) to a particular location at a given time. This can happen in one of two ways: (i) the suspect's fingerprints are taken and cross-matched with those fingerprints found at the scene of a crime; or (ii) a successful match is found using computer technology to compare the fingerprints found at the scene of a crime with a database of previous offenders. It should be noted that fingerprinting in criminal law is not new. Manual standards, for instance, existed since the 1920s when the Federal Bureau of Investigation (FBI) in the U.S. started processing fingerprint cards. These standards ensured completeness, quality and permanency.

By the early 1970s due to progress in computer processing power and storage, and the rise of new more sophisticated software applications, law enforcement began to use automatic machines to classify, store, and retrieve fingerprint data. The FBI led the way by introducing the Integrated Automated Fingerprint Identification Systems (IAFIS) that could scan a fingerprint image and convert the minutiae to digital information and compare it to thousands of other fingerprints [5, p.411]. Today, very large computer databases containing millions of fingerprints of persons who have been arrested are used to make comparisons with prints obtained from new crime scenes. These comparisons can literally take seconds or minutes depending on the depth of the search required. Sometimes successful matches can be made, other times the fingerprints cannot be matched. When fingerprints cannot be matched it is inferred that a new offender has committed a crime. These 'new' prints are still stored on the database as a means to trace back crimes committed by a person committing a second offence and who is apprehended by direct evidence, thus creating a trail of criminal events linked back to the same individual with the potential to solve multiple crimes. Commonly a list of prints that come closest to matching that print found at the scene of a crime are returned for further examination by an expert who then deems which single print is the closest match. In recent years background checks are even conducted on individuals using fingerprints, as a means to gain employment such as in early childhood [4, p.5], or during the process of adoption or other security clearance requirements.

5. What is DNA?

DNA fingerprinting, DNA (geno)typing, DNA profiling, identity testing and identification analysis, all denote the ability to characterize one or more rare features of an individual's genome, that is, their hereditary makeup. DNA contains the blueprints that are responsible for our cells, tissues, organs, and body [4, p.8]. In short it can be likened to "God's signature" [6, p.259]. Every single human has a unique composition, save for identical twins who share the same genotype but have subtly different phenotypes. When DNA samples are taken from blood cells, saliva or hair bulb specimens of the same person, the structure of the DNA remains the same. Thus only one sample is required as the basis for DNA profiling, and it can come from any tissue of the body [7, p.1]. DNA fingerprinting was discovered in 1985 by English geneticist Dr Alec Jeffreys. He found that certain regions of DNA contained sequences that repeated themselves over and over again, one after the other and that different individuals had a different number of repeated sections. He developed a technique to examine the length variation of these DNA repeat sequences, thus creating the ability to perform identification tests [8, pp.2f].

The smallest building block of DNA is known as the nucleotide. Each nucleotide contains a deoxyribose, a phosphate group and a base. When we are analyzing DNA structures it is the sequence of bases that is important for the purposes of identification [9, p.11]. There are four bases through which a genetic code is described. These are: Adenine (A), Thymine (T), Guanine (G) and Cytosine (C). When trying to understand DNA sequences as they might appear in written form, consider that 'A' only binds with 'T', and 'G' only binds with 'C' (see figure 2 comparing row one and two). These base pairs are repeated millions of times in every cell and it is their order of sequence that determines the characteristics of each person. It is repetitive DNA sequences that are utilized in DNA profiling [10, p.2].

5'-CTTAGCCATAGCCTA-3'
3'-GAATCGGTATCGGAT-5'

Figure 2. A Typical DNA Sequence

For example, in Figure 2 the base sequences of the two strands, known as the double helix, is written for a fictitious DNA sample. While the labels "5" and "3" have been included for illustrative purposes a sequence is written plainly as CTTAGCCATAGCCTA. From this sequence we can deduce the second strand given the rules for binding described above. Furthermore, in specific

applications of DNA testing various polymorphisms may be considered which denote the type of repeat for a given stretch of DNA. For instance the tetranucleotide repeat is merely a stretch of DNA where a specific four nucleotide motif is repeated [9, p.10].

5.1. DNA as Applied to Criminal Law

DNA profiling can be applied to a broad range of applications including diagnostic medicine, family relationship analysis (proof of paternity and inheritance cases), and animal and plant sciences [7, p.31]. The most high profile use of DNA however is in the area of forensic science, popularized by modern day television series such as CSI Miami and Cold Case. Episodes from the series, such as "Death Pool" [11] and "Dead Air," [12] allow members of the public to visualize how DNA might be used to gather evidence towards prosecution in a court of law. Although Hollywood is well known for its farcical and inaccurate representations, these episodes still do demonstrate the potential for DNA. DNA profiling illustrates the power to eliminate a suspect with a discrimination power so high that it can be considered a major identification mechanism [13, p.1]. It is with no doubt that forensic DNA analysis has made a huge impact on criminal justice and the law since its inception in U.K. Courts with the 1988 investigation into the deaths of schoolgirls Lynda Mann in 1983 and Dawn Ashworth in 1986 [14]. Since that time, DNA has been used successfully in criminal law to help prove guilt or innocence [15], in family law to prove parentage, and in immigration law to prove blood relations for cases related to citizenship [4, p.xiii].

In forensic DNA analysis today, mitochondrial DNA is used for identification, as nuclear DNA does not possess the right properties toward individual identification [9, p.5]. According to Koblinsky et al. it is the moderately repetitious DNA that is of interest to forensic analysts [4, pp.17f]:

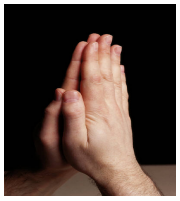
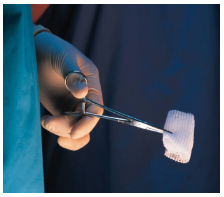
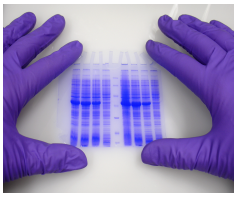
> "It has been shown that 99.9% of human DNA is the same in every individual. In fact, every individual's DNA has a relatively small number of variations from others. It is that variation of 1 in every 1000 bases that allows us to distinguish one individual from another through forensic genetic testing."

Similarly in the case of dactyloscopy, an individual's DNA can be left behind at a scene of a crime or on a victim. When natural fibers are transferred through human contact, for example, from a perpetrator to a victim, or natural fibers sometimes microscopic in nature are left behind at a scene of a crime, they can be used for evidentiary purposes. The DNA found in hair for example, can be compared to hair specimens taken from a crime suspect or the DNA profile stored in an existing DNA databank. Synthetic fibers not containing DNA, such as threads from a piece of clothing worn by a perpetrator, can also be used to link a suspect to a crime. When fibers are transferred from one person to another upon physical contact it is known as the Locard exchange principle [4, p.3].

It is important to note that all physical evidence like DNA should only ever be considered circumstantial evidence. It is evidence that provides only a basis for inference about the claim being made, and can be used in logical reasoning to prove or disprove an assertion. In a criminal case, DNA alone cannot be used to prove someone's guilt or innocence. Rather DNA may be able to point investigators to 'what happened', 'the order of events that took place', 'who was involved', 'where an event took place' and 'how it might have taken place,' and in that manner the forensic scientist is conducting a reconstruction by means of association (table 1) [16, p.1]. Thus the job of an investigator is to put all the pieces of the puzzle together and to gather as much information as possible and from as many available sources of evidence including eyewitness accounts, physical evidence and archival records [4, p.1].

Table 1. A Theoretical Framework for the Discipline of Criminalistics [16, p.2]

1.	Divisible matter: the division of matter
2.	Transfer: the exchange of material between two objects
3.	Identification: the physico-chemical nature of evidence
4.	Individualization: determine the source of the evidence
5.	Association: linking a person with a crime scene
6.	Reconstruction: understanding the sequence of past events.

As more sophisticated techniques have emerged to analyze DNA samples taken at the scene of a crime, the lesser the mass of DNA that is needed for a correct reading. How much DNA do you need? Well, it all depends on the richness of the sample. For instance, a 2002 US State Police handbook noted that a clump of pulled hair contained enough material for successful RFLP (Restriction Fragment Length Polymorphism) typing. A single hair root provided enough nuclear DNA for PCR STR (polymerase chain reaction short tandem repeat) typing, but not enough for RFLP. And a hair shaft contained sufficient mitochondria for successful mtDNA (mitochondrial DNA) typing, but was inadequate for PCR STR or RFLP typing [16, p.61]. A blood, saliva, urine, bone, teeth, skin or semen sample could be considered a richer sample than a hair root for extraction purposes, but

DNA analysis is all very much dependent on the level of degradation the sample has been exposed to.

Environmental factors can be harmful to DNA that has been collected from a scene of a crime and can lead to issues relating to deterioration, destruction, or contamination of evidence which are all contestable issues a lawyer may have to deal with in a court of law [4, p.xiii]. For instance, heat, moisture, bacteria, ultraviolet (UV) rays and common chemicals can contribute to the degradation process [9, p.61]. When a sample undergoes some level of degradation, it is said to have had infringed upon the chain of custody. To get around such problems, experts have proposed bringing the laboratory closer to policing practice. The concept of "lab in a van" or "lab on a chip" (LOC) proposes the use of a mobile laboratory where analysis and interpretation of evidence is even possible at the scene of a crime [6, p.153]. The advancements in mobile technologies continue to allow for even very tiny biological substances to undergo DNA testing resulting in accurate identification. Even a cigarette butt which has saliva on it containing epithelial cells can be screened for DNA evidence [4, p.6].

6. Comparing DNA and Fingerprinting

To begin with, traditional fingerprinting classification techniques have been around a lot longer than DNA identification, although both fingerprinting and DNA have been part of the human body since the start of time. In its manual form, the Galton-Henry system of fingerprint classification first made its impact on the practices of Scotland Yard in 1901. So whereas fingerprint recognition can happen using manual methods, DNA testing can only happen using laboratory systems, even if analysis now takes the form of a mobile lab on a chip. DNA is also a pervasive and invasive biometric technique. That is DNA is owned by everyone, and DNA actually belongs to the internals of what makes up the body. For a DNA reading, a hair shaft has been detached from the scalp, teeth and skin and bones have to be 'dismembered' from the body, blood and urine and saliva is extracted from the body [17, p.374].

In most states, the police can take non-intimate samples if a person has been arrested for a serious recordable offence, and in other states DNA can be taken for offences such as begging, being drunk and disorderly, and taking part in an illegal demonstration. In the U.K. for instance, DNA does not have to be directly relevant to investigating the offence for which a person is being arrested and they do not have to be charged before the sample is taken. The police are not allowed to take more than one successful sample from the same body part during the course of an investigation. The police can take an intimate sample only with a person's written consent even if they have been arrested. However, there is a burgeoning debate at present about what actually constitutes consent during such a process- is it true consent, or merely compliance or acknowledgment of required police procedures by the individual under arrest.

Fingerprints are different in that while belonging to the body, they are a feature on the surface of the body, and they do not constitute mass. Fingerprints are patterns that appear on the skin, but they are not the fiber we know as skin. Fingerprints also exclude a small portion of the population- those who do not have particular fingers, or hands, or arms, or may have fingers that have been severely deformed due to accidental or deliberate damage. Despite these differences, the claim is made by scientists that forensic DNA testing has emerged as an accurate measure of someone's identification with reliability equal to that of fingerprint recognition [4, p.5].

6.1. Intimate and Non-Intimate Measures: Other Biometrics versus DNA Sampling

6.1.1. The United States and Other Biometrics. The notion of "intimacy" is very much linked to literature on DNA, and not of biometrics in general. Although historically there has been some contention that a fingerprint sample is both "intimate" and "private", the proliferation of fingerprint, handprint, and facial recognition systems now used for government and commercial applications, has rendered this debate somewhat redundant. This is not to say that the storage of personal attributes is not without its own commensurate risks but large-scale applications enforced by such acts as the United States *Enhanced Border Security and Visa Entry Reform Act of 2002* mean that fingerprint, hand and facial recognition systems have now become commonplace. In fact, this trend promises to continue through multimodal biometrics, the adoption of several biometrics toward individual authentication. Few travelers, at the time of transit, directly challenge the right of authorities to be taking such personal details, and to be storing them on large databases in the name of national security. However sentiment, at least in North America, was different prior to the September 11 terrorist attacks on the Twin Towers [18].

In 1997 biometrics were touted a type of personal data which was wholly owned by the individual bearer with statutory implications depending on the governing jurisdiction [19]. It followed that a mandatory requirement by a government agency to collect and store fingerprint data may have been in breach of an individual's legitimate right to privacy. In the U.S., court cases on this issue have found consistently that certain biometrics do not violate federal laws like the Fourth Amendment. It seems that the [20]:

> "…real test for constitutionality of biometrics… appears to be based on the degree of physical intrusiveness of the biometric procedure. Those

that do not break the skin are probably not searches, while those that do are".

In the context of DNA we can almost certainly claim that there is "physical intrusiveness" of a different nature to the collection of surface-level fingerprints (figure 2). In the collection of blood samples we must "break" or "pierce" the skin, in the collection of saliva samples we enter the mouth and touch the inner lining of the mouth with buccal swabs, in the removal of a hair or clump of hair we are "pulling" the hair out of a shaft etc. And it is here, in these examples, where consent and policing powers and authority become of greatest relevance and significance.

Figure 2. Left: Finger "prints" on the surface of the skin. Right: DNA blood "sample" taken by pricking the skin

6.1.2. Britain and DNA. In the world of DNA, there is a simple classification, followed by most law enforcement agencies that denote samples as either being of an "intimate" nature or "non-intimate" nature. In the British provisions of the original *Police and Criminal Evidence Act of 1984* (PACE), section 65 defines intimate samples as: "a sample of blood, semen or any other tissue fluid, urine, saliva or pubic hair, or a swab taken from a person's body orifice" and non-intimate samples as "hair other than pubic hair; a sample taken from a nail or from under a nail; a swab taken from any part of a person's body other than a body orifice" [21, p.80]. Generally, it must be noted that at times police can take a sample by force but on other occasions they require consent. In Britain, prior to 2001, intimate samples from a person in custody were once only obtainable through the express authority of a police officer at the rank of superintendent and only with the written permission of the person who had been detained (section 62) [21]. Non-intimate samples could be taken from an individual without consent but with permission from a police officer of superintendent rank (section 63). In both instances, there had to be reasonable grounds for suspecting that the person from whom the sample would be taken had been involved in a serious offence [21]. And above reasonable grounds, there had to be, theoretically at least, the potential to confirm or disprove the suspect's involvement through obtaining a DNA sample [22, p.29]. Over time Acts such as the PACE have been watered down leading to controversial strategic choices in law enforcement practices, such as the trend towards growing national DNA databases at a rapid rate.

6.2. Continuity of Evidence

Policing and forensic investigative work, are no different to any other "system" of practice; they require to maintain sophisticated audit trails, even beyond those of corporate organizations, to ensure that a miscarriage of justice does not take place. However, fingerprints are much easier attributes to prove a continuity of evidence than DNA which is much more complex. A fingerprint found at a crime scene, does not undergo the same type of degradation as a DNA sample. Thus it is much easier to claim a fingerprint match in a court of law, than a DNA closeness match. Providing physical evidence in the form of a DNA sample or profile requires the litigator to prove that the sample was handled with the utmost of care throughout the whole chain of custody and followed a particular set of standard procedures for the collection, transportation, and handling of the material. The proof that these procedures were followed can be found in a series of paper trails which track the movements of samples [6, p.114].

Beyond the actual location of the evidence, a continuity of evidence has to do with how a DNA sample is stored and handled, information related to temperature of the place where the sample was found and the temperature at the place of storage, whether surrounding samples to that being analyzed were contaminated, how samples are identified and qualified using techniques such as barcode labels or tags, how samples were tested and under what conditions, and how frequently samples were accessed and by whom and for what purposes [4, p.43]. When DNA forensic testing was in its infancy, knowledgeable lawyers would contest the DNA evidence in court by pointing to micro-level practices of particular laboratories that had been tasked with the analytical process. The first time that attention had been focused on the need to standardize procedures and to develop accreditation processes for laboratories and for personnel was in the 1989 case *People v Castro 545 N.Y.S.2d 985 (Sup. Ct. 1989)*. When DNA testing began it was a very unregulated field, with one commentator famously noting that: "clinical laboratories [were required to] meet higher standards to be allowed to diagnose strep throat than forensic labs [were required to] meet to put a defendant on death row" [9, p.55]. But it must be said, given the advancement in quality procedures, attacks on DNA evidence, rarely focus on the actual standards, and more so focus on whether or not standards were followed appropriately [9, p.61].

In the event that a defense lawyer attempts to lodge an attack on the DNA evidence being presented in a court of law, they will almost always claim human error with respect to the procedures not being followed in

accordance to industry standards. Human error cannot be eradicated from any system, and no matter how small a chance, there is always the possibility that a sample has been wrongly labeled or contaminated with other external agents [9]. Worse still is the potential for a forensic expert to provide erroneous or misleading results, whether by a lack of experience, a miscalculation on statistical probabilities or deliberate perjury. The latter is complex to prove in court. Some have explained away these human errors toward wrongful conviction as a result of undue political pressure placed on lab directors and subsequently analysts for a timely response to a violent crime [16, p.157]. As Michaelis et al. note [9, p.69]:

> "[i]n far too many cases, the directors of government agencies such as forensic testing laboratories are subjected to pressure from politicians and government officials to produce results that are politically expedient, sometimes at the expense of quality assurance… Laboratory directors are too often pressured to produce results quickly, or to produce results that will lead to a conviction, rather than allowed to take the time required to ensure quality results."

Thus attacks on DNA evidence can be made by attacking the chain of custody among other strategies shown in Table 2.

Table 2. Ways to Mitigate the Effect of DNA Evidence

- New type of DNA test
- Expert not qualified to testify as to DNA results
- Laboratory not accredited
- Testing not performed by certified technicians
- Lack of discovery material or notice with respect to the admission of DNA evidence
- Improperly obtained DNA evidence
- DNA profile should have been purged from database
- Expert not qualified to testify as to statistics
- Statistics do not conform to standards accepted by the scientific community
- Irrelevant/improper database use
- Expert not qualified to testify as to statistics in context opinion is being offered
- Attacking laboratory techniques and conditions
- Attacking DNA test used
- Attacking chain of custody
- Attacking expert witness
- Contamination
- Attacking the choice not to employ several different DNA tests, including sequencing
- Preventing testimony regarding the ultimate issue
    - o DNA evidence is useful for exclusion, it cannot identify with certainty
    - o Objecting to testimony regarding defendant's guilt

7. The Difference between Databases and Databanks

7.1. Of Profiles and Samples

In almost any biometric system, there are four steps that are required towards matching one biometric with another. First, data is acquired from the subject, usually in the form of an image (e.g. fingerprint or iris). Second, the transmission channel which acts as the link between the primary components will transfer the data to the signal processor. Third, the processor takes the raw biometric image and begins the process of coding the biometric by segmentation which results in a feature extraction and a quality score. The matching algorithm attempts to find a record that is identical resulting in a match score. Finally, a decision is made based on the resultant scores, and an acceptance or rejection is determined [23]. At the computer level, a biometric image is translated into a string of bits, that is, a series of one's and zero's. Thus a fingerprint is coded into a numeric value, and these values are compared in the matching algorithm against other existing values. So simply put, the input value is the actual fingerprint image, and the output value is a coded value. This coded value is unique in that it can determine an individual profile.

With respect to the extraction of a DNA sample the process is much more complex, as is its evaluation and interpretation. A DNA sample differs from a fingerprint image. A sample is a piece of the body or something coming forth or out from the body, while in the case of fingerprints, an image is an outward bodily aspect. When a DNA sample undergoes processing, it is also coded into a unique value of As, Ts, Gs and Cs. This value is referred to as a DNA profile. Storing DNA profiles in a computer software program is considered a different practice to storing the actual feature rich DNA sample in a DNA store. Some members of the community have volunteered DNA samples using commercial DNA test kits such as "DNA Exam" by the BioSynthesis Corporation [24]. For example, the DNA Diagnostics Center [25] states that one may:

> "…elect to take advantage of [the] DNA banking service without any additional charge if [one] orders a DNA profile [and that the company] will store a sample of the tested individual's DNA in a safe, secure facility for 15 years—in case the DNA sample is ever needed for additional testing".

The controversy over storing "samples" by force in the crime arena has to do with the potential for DNA to generate information such as a person's predisposition to disease or other characteristics that a person might consider confidential. It is the application of new algorithms or extraction/ evaluation/ interpretation techniques to an existing sample that is of greatest

concern to civil liberties advocates. Profiles are usually unique combinations of 16 markers [26], they can only be used to match, and cannot be used toward further fact finding discoveries although some believe that you might be able to draw conclusions from profiles in the future. In a given population, there are several different alleles for any single marker and some of these may appear more frequently than others. The best markers are those with the greatest number of different alleles and an even distribution of allele frequencies [9, p.19].

7.2. Of Databases and Databanks

Although textbooks would have us believe that there is a clear-cut distinction about what constitutes a database as opposed to a databank, in actual fact the terms are used interchangeably in most generalist computing literature. Most dictionaries for example will define the term *database* without an entry for *databank*. A database is a file of information assembled in an orderly manner by a program designed to record and manipulate data and that can be queried using specific criteria. Commercial enterprise grade database products include Oracle and Microsoft Access. The International Standards Organization however, does define a databank as being "a set of data related to a given subject and organized in such a way that it can be consulted by users" [27]. This distinction is still quite subtle but we can extrapolate from these definitions that databases are generic information stores, while databanks are specific to a subject [28].

In the study of DNA with respect to criminal law, the distinction between databases and databanks is a lot more crystallized, although readers are still bound to be confused by some contradictory statements made by some authors. Still, in most cases, a databank is used to investigate crimes and to identify suspects, and a database is used to estimate the rarity of a particular DNA profile in the larger population [9, p.99]. Databanks contain richer personal information related to samples, even if the identity of the person is unknown. For example, the databank can contain unique profiles of suspects and convicted criminals and content about physical crime stains and records of DNA profiles generated by specific probes at specific loci [10, p.40]. Databases are much more generic than databanks containing information that is representative of the whole populace or a segment of the populace. For example, a database can contain statistical information relating to the population frequencies of various DNA markers generated from random samples for particular ethnic groups or for the whole population at large. Databanks may contain rich personal data about offenders and cases [16, pp.157f] but databases only contain minimal information such as the DNA profile, ethnic background and gender of the corresponding individuals.

The premise of the DNA databank is that DNA profile data of known offenders can be searched in an attempt to solve crimes, known as 'cold cases'. They are valuable in that they can help investigators string a series of crimes together that would otherwise go unrelated, allowing for the investigator to go across space and time after all other avenues have been exhausted [9, p.99]. With respect to violent crimes, we know that offenders are highly prone to re-offending and we also know that violent crimes often provide rich DNA sample sources such as bones, blood, or semen. Thus DNA left at the scene of a crime can be used to search against a DNA databank in the hope of a "close" match [16, p.157]. The probative value of the DNA evidence is greater the rarer the DNA profile in the larger population set [9, p.19].

Table 3. The NDNAD Database Attributes [30]

- Unique barcode reference number linking it to the stored DNA sample
- Arrest Summons Number, which links it to the record on the Police National Computer (PNC) containing criminal records and police intelligence information;
- the person's name, date of birth, gender and "ethnic appearance" (as assigned by a police officer);
- information about the police force that collected the sample;
- information about the laboratory that analyzed the sample;
- sample type (blood, semen, saliva, etc);
- test type;
- DNA profile as a digital code.

Different jurisdictions have different standards on the criteria for inclusion into DNA databanks and what attribute information is stored in individual records and who has access. In the United States for instance, different states have different rules, some allowing for DNA databanks to be accessed by law enforcement agencies alone, and others allowing for public officials to have access for purposes outside law enforcement [9, p.100]. In the U.S. the CODIS (Combined DNA Index System) system was launched in 1998-99 by the FBI. It contains two searchable databases, one with previous offenders and another with DNA profiles gathered from evidence at crime scenes [9, p.16]. In the case of the U.K., the National DNA Database (NDNAD) of Britain, Wales and Northern Ireland, contains very detailed information for each criminal justice (CJ) record (see table 3) and profiles are searched against each other on a daily basis with close hit results forwarded on to the appropriate police personnel. It is quite ironic that the 1995 NDNAD is a databank but is so large that it is considered a database by most, as is also evident by the fact that the word "database" also appears in the NDNAD acronym [29, p.2].

8. Legal, Ethical and Social Concerns

The collection, storage, and use of DNA samples, profiles and fingerprints raise a number of legal, ethical and social concerns. While some of the concerns for the collection and storage of an individual's fingerprints by the State have dissipated over the last decade, the debate over the storage of DNA samples and profiles rages more than ever before. It was around the turn of the century when a number of social, ethical and legal issues were raised with respect to DNA sampling but councils and institutes through lack of knowledge or expertise could hardly offer anything in terms of a possible solution or way forward to the DNA controversy [31, p.34]. At the heart of the techno-legal "controversy" is a clash of ideals coming from a collision of disciplines. For many medical practitioners working on topics related to consent or confidentiality, the legal position on DNA is one which acts as a barrier to important medical research. While few would dispute the importance of data protection laws and the ethical reasons behind balancing the right to privacy against other rights and interests, some in the medical field believe that the law has not been able to deal with exceptions where the use of DNA data could be considered proportionate, for instance, in the area of epidemiology. There are those like Iverson who argue that consent requirements could be relaxed for the sake of the common good.

> "We are not arguing that epidemiological research should always proceed without consent. But it should be allowed to do so when the privacy interference is proportionate. Regulators and researchers need to improve their ability to recognize these situations. Our data indicate a propensity to over-predict participants' distress and under-predict the problems of using proxies in place of researchers. Rectifying these points would be a big step in the right direction" [32, p.169].

Thinking in this utilitarian way, the use of DNA evidence for criminal cases, especially violent crimes, is something that most people would agree is a legitimate use of technology and within the confines of the law. The application of DNA to assist in civil cases, again, would seem appropriate where family and state-to-citizen disputes can only be settled by the provision of genetic evidence. Volunteering DNA samples to appropriate organizations and institutions is also something that an individual has the freedom to do, despite the fact that a large portion of the population would not participate in a systematic collection of such personal details. Voluntary donation of a DNA sample usually happens for one of three reasons: (i) to assist practitioners in the field of medical research; (ii) to assist in DNA cross-matching exercises with respect to criminal cases; and (iii) to aid an individual in the potential need they may have of requiring to use their own DNA in future uses with any number of potential possibilities. For as Carole McCartney reminds us:

> "[f]orensic DNA technology has multiple uses in the fight against crime, and ongoing research looks to expand its usefulness further in the future. While the typical application of DNA technology in criminal investigations is most often unproblematic, there needs to be continued vigilance over the direction and implications of research and future uses" [33, p.189].

It is in this parallel development that we can see an evolution of sorts occurring with the collection of highly intimate personal information. On the one hand we have the law, on the other hand we have medical discovery, both on parallel trajectories that will have overflow impact effects on one other. For many, the appropriate use of DNA in the medical research field and criminal law field can only have positive benefits for the community at large. There is no denying this to be the case. However, the real risks cannot be overlooked. Supplementary industries can see the application of DNA in a plethora of programs, including the medical insurance of 'at risk' claimants to an unforeseen level of precision, measuring an individual's predisposition to a particular behavioral characteristic for employment purposes [34, p.897], and the ability to tinker with the genes of unborn children to ensure the "right" type of citizens are born into the world. All of these might sound like the stuff of science fiction but they are all areas under current exploration.

For now, we have the ability to identify issues that have quickly escalated in importance in the DNA debate. For this we have several high profile cases in Europe to thank but especially the latest case which was heard in the European Court of Human Rights (ECtHR) on the 4 December 2008, that being *S and Marper v. the United Kingdom* [35]. This landmark case, against all odds, acted to make the U.K. (and to some extent the rest of the world) stop and think about the course it had taken. For the U.K. this meant a re-evaluation of its path forward via a community consultation process regarding the decade old initiatives of the NDNAD. The main issues that the case brought to the fore, and those of its predecessor cases, can be found in summary in Table 4. The table should be read from left to right, one row at a time. The left column indicates what most authors studying the socio-ethical issues regard as an acceptable use of DNA, and the right column indicates what most authors regard as either debatable or unacceptable use of DNA.

Of greatest concern to most civil libertarians is the issue of proportionality and the potential for a disproportionate number of profiles to be gathered relative to other state practices towards a blanket coverage databank. Blanket coverage databanks can be achieved by sampling a populace, a census approach is not required. Maintaining DNA profiles for some 15-20% of the total population, means you could conduct familial searching

on the rest to make associations between persons with a high degree of accuracy [4, p.274], something that would be possible in the U.K. by 2018 if it maintained the same level of sampling due process. This is not without its dangers, as it promotes adventitious searching and close matches that might not categorically infer someone's guilt or innocence.

Table 4. Legal, Ethical and Social Issues Related to Use of DNA in Criminal Law

Acceptable →	**Debatable/Unacceptable**
Consent to DNA sample being taken	DNA sample taken by force
DNA sample taken only when charged	DNA sample taken on arrest
DNA profile retained only	DNA sample and profile retained
DNA sample retained for defined period	DNA sample retained indefinitely
DNA sample of adults retained only	DNA sample of a minor retained
DNA sample taken for violent crimes	DNA sample taken for minor offences and violent crimes
DNA data bank limited in scope	DNA data bank too large for intended use
DNA data bank anonymized	DNA data includes personal details
DNA profile for use by law enforcement	DNA sample for use by other public officials
DNA data bank is diverse	DNA data bank targets ethnic minorities
DNA profile used to cross-match only	DNA sample considered for future use
DNA profile used to identify a suspect	DNA profile used for familial searching
DNA samples of innocents destroyed	DNA samples of innocents retained
Conviction based on multiple sources	Conviction based on DNA evidence alone
DNA following a chain of custody	DNA interpretation of a degraded sample
Authorized access to DNA data bank	Unauthorized access to DNA data bank
Accredited laboratory for DNA processing	Off-shoring DNA data storage and processing
Multiple authorities accountable for DNA	One authority/agency accountable for DNA
DNA analysis following quality practice	Involvement of politicians in scientific process

In addition, the large databanks are not without their bias. Already police records are filled with the presence of minority groups of particular ethnic origin for instance, which can have an impact on the probability of a close match despite someone's innocence. Being on the database means that there is a chance a result might list you as a suspect based on having a similar DNA profile to someone else. And ultimately, the fact that innocent people would have their profiles stored on the NDNAD would do little in the way of preventing crime, and would lead before too long, to a de facto sampling of all state citizens.

The driving force behind such a campaign could only be achieved by obtaining DNA samples from persons (including innocent people or 'innocents'), either via some event triggering contact between an individual and the police or via an avenue at birth [10, p.40]. Police powers have increased since world wide terrorist attacks post 2000 especially, and this has led to a tradeoff with an individual's right to privacy [36, p.14]. Notions of consenting to provide a DNA sample to law enforcement personnel have been challenged whereby the use of force has been applied. And not consenting to a sample being taken, even if you are innocent has its own implications and can be equally incriminating. So legislative changes have encroached on individual rights; whereby a warrant was once required to take a DNA sample from a suspect's body based on reasonable grounds, today it is questionable if this caveat actually exists.

Beyond the obvious downsides of retaining the DNA profile or sample of innocent people who are in actual fact law abiding citizens, there is the potential for persons to feel aggravated because they have not been let alone to go about their private business. Innocent persons who are treated like criminals may end up losing their trust in law enforcement agencies. This problem is not too small of a social issue, given that there are about 1 million innocent people on the NDNAD in the U.K. And in this context, it is not difficult to see how some individuals or groups of individuals might grow to possess an anti-police or anti-government sentiment, feeling in some way that they have been wronged or singled out. In some of these 'mistaken identity' situations, surely it would have been better to prove someone's innocence by using other available evidence such as closed circuit television (CCTV), without the need to take an intimate DNA sample first. Despite these problems, it seems anyone coming under police suspicion in the U.K. will have their DNA taken anyway [33, p.175].

Of a most sensitive nature is the collection of DNA samples for an indefinite period of time [4, p.7]. In most countries, samples are taken and DNA profiles are determined and stored in computer databases, and subsequently samples are destroyed. The long-term storage of DNA samples for those who have committed petty crimes and not violent crimes raises the question of motivation for such storage by government authorities [4]. There are critics who believe that the retention of samples is "an unjustifiable infringement on an individual's privacy" [33, p.189].

Table 5. Social, Ethical and Legal Issues Pertaining to DNA Databanks Identified by National Institute of Justice in the United States in 2000 [31, pp. 35f].

1. Group and trait identification: Thus, a particular profile in a crime scene sample may be more probably in one group than in another. There is already much public discussion of "racial profiling." *2. Identification of relatives:* With 13 STR loci it is quite likely that a search of a database will identify a person who is a relative of the person contributing the evidence sample. Suppose a crime scene profile shows a partial match with someone in the database. Are law enforcement officers entitled to investigate the relatives? *3. Broadening the database:* The largest database at present is that of convicted felons, usually perpetrators of major crimes. There is considerable interest in increasing the database to include persons convicted of lesser crimes or arrestees. In Britain everyone arrested for offenses that would lead to prison terms if convicted has a DNA sample taken at the time of arrest, but the profile is removed from the database if the person is not convicted. Inevitably, there will be the increasing possibility of broadening the database to include the general public. There would be many advantages, such as identification of persons or body parts after accidents, or discovery of kidnapped or lost people. At the same time, the risk to individual privacy would be enhanced and protection of anonymity would be harder. Balancing benefits and risks of population databases will continue to be a contentious issue in the future. *4. Saving DNA samples:* At present, there is no clear overall policy as to what happens to the DNA sample after profiles are added to the database, but the majority of States now have sample storage policies. It can be argued that saving the DNA permits retesting and inclusion of additional loci, particularly newly discovered ones. This would be much more efficient than searching out the person, who may not even be living. On the other side, it is argued that the profiles are recorded and that this information is all that is needed, not the DNA itself. Furthermore, those fearful of invasion of privacy are concerned lest the DNA become available to unauthorized parties or otherwise be used in ways that would disclose information that ought to remain confidential. *5. Use of CODIS database for research:* As the database enlarges and if it is broadened to include persons convicted of a larger variety of crimes, it might be possible that statistical studies of the databases cold reveal useful information.

Caption: There is much that has changed with respect to social, ethical and legal issues since 2000, both in the United States and the United Kingdom since its publication. But the table still provides a historical insight into the growing list of issues that were identified at the turn of the century.

Equally alarming is the storage of samples of innocents and also of those who are minors. Even more disturbing is the storage of samples with which no personal details have been associated. DNA databanks are not different to other databanks kept by the state- they can be lost, they can be accessed by unauthorized persons, and results can be misrepresented either accidentally or deliberately [33, p.188]. The stakes however are much higher in the case of DNA than in fingerprinting or other application areas because the information contained in a DNA sample or profile is much richer in potential use. All of this raises issues pertaining to how changes in the law affect society, and how ethics might be understood within a human rights context.

9. Conclusion

The legal, social and ethical issues surrounding the collection, use and storage of DNA profiles and samples is probably more evident today than at any other time in history. On the one hand we have the necessity to advance technology and to use it in situations in which it is advantageous to the whole community, on the other hand this same technology can impinge on the rights of individuals (if we let it), through sweeping changes to legislation. Whether we are discussing the need for DNA evidence in criminal law, civil law, epidemiological research or other general use, consent should be the core focus of any and every collection instance. Unlimited retention of DNA samples collected from those arrested but not charged is another issue where legislative reforms need to be taken in a number of European jurisdictions, although this trend seems to be gathering momentum now more so outside Europe. Another issue is the redefinition of what constitutes an intimate or non-intimate sample, and here, especially most clearly we have a problem in a plethora of jurisdictions with regards to the watering down of what DNA procedures are considered invasive as opposed to non-invasive with respect to the human body. The bottom line is that we can still convict criminals who have committed serious recordable offences, without needing to take the DNA sample of persons committing petty crimes, despite that statistics allege links between those persons committing serious and petty offences. So long as a profile is in a database, it can be searched, and the problem with this is that so-called 'matches' (adventitious in nature) can be as much 'incorrect' as they are 'correct'. And this possibility alone has serious implications for human rights. The time to debate and discuss these matters is now, before the potential for widespread usage of DNA becomes commonplace for general societal applications.

10. Afterword

Although members of society should not expect to learn of a black market for DNA profiles just yet, it is merely a matter of time before the proliferation and use of such profiles means they become more attractive to members of illicit networks. There is now overwhelming evidence to show that identity theft worldwide is on the rise (although estimates vary depending on the study and state). The systematic manipulation of identification numbers, such as social security numbers, credit card numbers, and even driver's license numbers for misuse is now well documented. Victims of identity theft know too well the pains of having to prove who they are to government agencies and financial institutions, and providing adequate evidence that they should not be held liable for information and monetary transactions they did not commit. Today's type of identity theft has its limitations however- stealing a number is unlike stealing somebody's *godly signature*. While credit card numbers can be replaced, one's DNA or fingerprints cannot. This resonates with the well-known response of Sir Thomas More to Norfolk in *A Man for All Seasons*: "…you might as well advise a man to change the color of his eyes [another type of biometric]", knowing all too well that this was impossible. While some have proclaimed the end of the DNA controversy, at least from a quality assurance and scientific standpoint, the real controversy is perhaps just beginning.

11. Acknowledgements

The author would like to acknowledge Associate Professor Clive Harfield of the Centre for Transnational Crime Prevention in the Faculty of Law at the University of Wollongong for his mentorship in the areas of U.K. law and policing in 2009. The author also wishes to extend her sincere thanks to Mr Peter Mahy, Partner at Howells LLC and the lawyer who represented S & Marper in front of the Grand Chamber at the European Court of Human Rights, for his willingness to share his knowledge on the NDNAD controversy via a primary interview.

12. References

[1] J. R. Parks, "Automated personal identification methods for use with smart cards," in *Integrated Circuit Cards, Tags and Tokens: new technology and applications*, P. L. Hawkes, Ed. Oxford: BSP Professional Books, 1990, pp. 92-135.

[2] A. K. Jain, L. Hong, S. Pankati, and R. Bolle, "An identity-authentication system using fingerprints," *Proceedings of the IEEE*, vol. 85, pp. 1365-1387, 1997.

[3] J. Cohen, *Automatic Identification and Data Collection Systems*. London: McGraw-Hill Book Company, 1994, p. 228.

[4] L. Koblinsky, T. F. Liotti, and J. Oeser-Sweat, "DNA: Forensic and Legal Applications." New Jersey: Wiley, 2005.

[5] P. T. Higgins, "Standards for the electronic submission of fingerprint cards to the FBI," *Journal of Forensic Identification*, vol. 45, pp. 409-418, 1995, p. 411.

[6] M. Lynch, S. A. Cole, R. McNally, and K. Jordan, *Truth Machine: the Contentious History of DNA Fingerprinting*. Chicago: The University of Chicago Press, 2008.

[7] L. T. Kirby, *DNA Fingerprinting: An Introduction*. New York: Stockton Press, 1990.

[8] J. M. Butler, *Forensic DNA Typing: Biology, Technology, and Genetic of STR Markers*. Amsterdam: Elsevier Academic Press, 2005, pp. 2f

[9] R. C. Michaelis, R. G. Flanders, and P. H. Wulff, *A Litigator's Guide to DNA: from the Laboratory to the Courtroom*. Amsterdam: Elsevier, 2008.

[10] C. A. Price, *DNA Evidence: How Reliable Is It? An Analysis of Issues Which May Affect the Validity and Reliability of DNA Evidence*, vol. 38: Legal Research Foundation, 1994.

[11] A. Donahue and E. Devine, "Death Pool (Season 5, Episode 3)," in *CSI Miami*, S. Hill, Ed., 2006.

[12] J. Haynes, "Dead Air (Season 4, Episode 21)," in *CSI Miami*, S. Hill, Ed., 2006.

[13] B. Selinger, "The Scientific Basis of DNA Technology," in *DNA and Criminal Justice*, vol. 2, J. Vernon and B. Selinger, Eds. Canberra: Australian Institute of Criminology, 1989.

[14] Reuters. (14 May 2009) Man jailed in first DNA case wins murder appeal, [Online]. Available: http://uk.reuters.com/article/idUKTRE54D3CC20090514?pageNumber=1&virtualBrandChannel=0

[15] (2009) The Innocence Project- Home, [Online]. Available: http://www.innocenceproject.org/

[16] N. Rudin and K. Inman, *An Introduction to Forensic DNA Analysis*, 2nd ed. London: CRC Press, 2002.

[17] A. Roberts and N. Taylor, "Privacy and the DNA Database," *European Human Rights Law Review*, vol. 4, 2005, p. 374.

[18] K. Michael and M. G. Michael, *Automatic Identification and Location Based Services: from Bar Codes to Chip Implants*: IGI, 2009.

[19] R. van Kralingen, C. Prins, and J. Grijpink. (1997) Using your body as a key; legal aspects of biometrics, [Online]. Available: http://cwis.kub.nl/~frw/people/kraling/content/biomet.htm

[20] S. O'Connor. (1998) Collected, tagged, and archived: legal issues in the burgeoning use of biometrics for personal identification, *Stanford Technology Law Review*. [Online]. Available: http://www.jus.unitn.it/USERS/pascuzzi/privcomp99-00/topics/6/firma/connor.txt

[21] S. Ireland, "What Authority Should Police Have to Detain Suspects to take Samples?," presented at DNA and Criminal Justice, Canberra, 1989, p. 80.

[22] I. Feckelton, "DNA Profiling: Forensic Science Under the Microscope," in *DNA and Criminal Justice*, vol. 2, J. Vernon and B. Selinger, Eds. Canberra: Australian Institute of Criminology, 1989, p. 29.

[23] K. Raina, J. D. Woodward, and N. Orlans, "How Biometrics Work," in *Biometrics*, J. D. Woodward, N. M. Orlans, and P. T. Higgins, Eds., 2002, pp. 29f

[24] BioSynthesis. (2009) Identity DNA Tests, [Online]. Available: http://www.800dnaexam.com/Identity_dna_tests.aspx

[25] DNA Diagnostics Center. (2009) Profiling, [Online]. Available: http://www.dnacenter.com/dna-testing/profiling.html

[26] Biosciences Federation and The Royal Society of Chemistry. (January 2007) Forensic Use of Bioinformation: A response from the Biosciences Federation and the Royal Society of Chemistry to the Nuffield Council on Bioethics, [Online]. Available: http://www.rsc.org/images/ForensicBioinformation_tcm18-77563.pdf

[27] J. C. Nader, "Data bank," in *Prentice Hall's Illustrated Dictionary of Computing*, 1998, pp. 152.

[28] Identigene. (2009) DNA Safeguarding for security and identification, [Online]. Available: http://www.dnatesting.com/dna-safeguarding/index.php

[29] The British Academy of Forensic Sciences. (2007) In response to the Nuffield Bioethics Council Consultation- The Forensic use of bioinformation: ethical issues between November 2006 and January 2007, [Online]. Available: http://www.nuffieldbioethics.org/fileLibrary/pdf/British_Academy_of_Forensic_Sciences.pdf

[30] Genewatch UK. (2009) What happens when someone is arrested?, [Online]. Available: http://www.genewatch.org/sub-539483

[31] National Institute of Justice, "The Future of Forensic DNA Testing: Predictions of the Research and Development Working Group," 2000.

[32] A. Iversen, K. Liddell, N. Fear, M. Hotopf, and S. Wessely, "Consent, confidentiality, and the Data Protection Act," *British Medical Journal*, vol. 332, 2006, p. 169.

[33] C. McCartney, "The DNA Expansion Programme and Criminal Investigation," *The British Journal of Criminology*, vol. 46, 2006, pp. 175, 189, 188.

[34] D. Meyerson, "Why Courts Should Not Balance Rights Against the Public Interest," *Melbourne University Law Review*, vol. 33, 2007, p. 897.

[35] Council of Europe, "Grand Chamber | Case of S. and Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04) Judgment," European Court of Human Rights, Strasbourg 4 December 2008.

[36] J. Kearney and P. Gunn, "Meet the Experts- Part III DNA Profiling," 1991, p. 14.