Irish Council for Civil Liberties
An Comhairle um Chearta Daonna

ICCL Position Paper

Human Rights Compatibility of the Establishment of a DNA Database

October 2003

Contents

The ICCL

The Irish Council for Civil Liberties (An Chomhairle um Chearta Daonna) is an independent non-governmental organisation that works to promote and defend human rights and civil liberties. It was founded in 1976 by, among others, Mary Robinson, Kader Asmal and Donal Barrington.

The ICCL draws on Ireland's international human rights commitments and the standards therein, as well as constitutional protections, to monitor government policy, campaign for reform and promote better compliance with international human rights norms.

The ICCL has actively campaigned in the area of criminal justice and equality and championed the rights of minorities including gay and lesbian rights, travellers' rights, women's rights, the rights of refugees and asylum-seekers. The ICCL has also specifically conducted several constitutional reform campaigns including around the referenda on abortion, bail and divorce..

For further details: **ICCL**
Dominick Court
40 – 41 Lower Dominick Street
Dublin 1
Telephone (01) 8783136
Fax: (01) 878 3109
E-mail: iccl@iol.ie
Web Site: http://www.iccl.ie

Executive Summary

- DNA profiling refers specifically to the biometric authentication of a person's identity via genetic traits of the individual. DNA information is capable of disclosing complex types of information about a person's family relationships, ethnic group and medical conditions. Continuous advances in science renders it impossible to predict the totality of information that could be revealed by a person's DNA. Some will even claim that genetic indicators exist for sexual orientation, substance addiction or even criminal inclination.

- The ICCL considers that the use of DNA and DNA profiling as a forensic tool in the detection and prosecution of crime offers many potential benefits and can be used in a positive way to establish the innocence of any suspect. The management of such use is critical to maximising the benefits and preventing abuse. The public must be confident that DNA is used in a manner which respects fundamental civil liberties and human rights, balances the requirements of criminal justice with the rights of the individual and efficiently and effectively uses state resources in the public interest.

- The ICCL favours a system of DNA use whereby DNA evidence from a crime scene can be compared only to the DNA profiles of suspects in the crime and opposes any system of mass screening with no reasonable cause. Examples from other jurisdictions reveal that there was no evidence that the mass screening had any causal link to the detection of perpetrators.

- Unlike the practice in some jurisdictions, the results of any DNA tests conducted in the course of an investigation must be available to all suspects as a means of establishing their innocence as well as to law enforcement agencies for the purpose of identifying a perpetrator.

- The ICCL considers that any proposed system of DNA *retention*, must be strictly justified in terms of the purpose of such retention and the actual effectiveness and efficiency in achieving the purpose by way of DNA retention. The ICCL questions whether there is statistical evidence in Ireland to support the need for comprehensive DNA retention over and above a practice of comparing DNA crime scene evidence to the DNA profile of suspects.

- The establishment and maintenance of a secure, high standard DNA retention system would require significant input of resources by the state. In light of the limited resources available to law enforcement agencies in the state, the value of using such resources on a DNA database as oppose to in other areas of crime detection and prosecution must be questioned in light of the volume of perpetrators of crime likely to be detected through reliance on a database.

- In order to be human rights compliant, any system of DNA retention particularly in the area of criminal justice, must be strictly limited in its purpose and must not be allowed to fall victim of the phenomenon of "function creep". It should be an explicit offence for a DNA database to be used for a purpose beyond that of suspect identification in criminal investigation.

- A system of DNA retention must also be restricted with respect to the persons whose DNA is retained and for how long so that the principles of presumption of innocence and fair trial are not compromised.

- As DNA profiling is capable of disclosing intimate and detailed information about a person, the far reaching privacy implications of DNA retention must be addressed. It must follow basic principles of data protection to ensure privacy, including stringent safeguards about who has access to the information, for

what purposes, and how long the information will be retained. There should be no sharing of the information with agencies outside those directly involved with law enforcement and the investigation and prosecution of a crime.

Introduction

1. DNA profiling is one of many means of authenticating a person's identity by biometric means. Biometric authentication and profiling technologies are based on the personal physiological characteristics of the individual. DNA profiling refers specifically to the genetic traits of the individual and its use has expanded greatly in recent years in line with dramatic advances in science.

2. As with all new technologies, DNA profiling offers both great potential for good while also carrying with it the potential for infringement of individual rights and freedoms. In the case of a DNA database however, we must address not just what potential pros and cons DNA profiling offers, but specifically what the implications are for the ***retention*** of DNA profiles. Any analysis of a proposed retention mechanism must involve a careful weighing up of the purported benefits of such a system against the risks and dangers such systems inevitably present. The fundamental principle of data retention, which runs through this paper, is that robust safeguards must be put in place before any system of data retention can be embarked upon that can enjoy the confidence and trust of a privacy-conscious public.

3. A common thread in the civil liberties perspective in this area is the phenomenon of 'function creep', whereby technology introduced for one narrowly defined purpose is extended in its usage over time to other areas. The principal danger is that invasive measures that might be deemed proportionate to achieve an important public interest objective later become used in other areas when the

original justification for those invasive measures has become obscured or forgotten.

4. In assessing the issues raised by this technology from a civil liberties perspective, we have looked at how traditional privacy concerns arise in relation to this new technology. However, DNA profiling and the use of DNA databases also raise several novel issues. The power of identification technology that is based on information of the person, rather than simply about the persons must always be borne in mind, as must the characteristic of DNA technology that it goes beyond strictly personal information to also present information about a person's family and ethnic group.

5. In this regard, references to DNA technology as a 'genetic fingerprint' are misleading. Fingerprints are two-dimensional representations with use solely for identification purposes. DNA information, on the other hand, is capable of disclosing complex types of information about a person's family relationships, the workings of a person's body and even the likelihood of a person suffering from a wide range of diseases. Some will even claim that genetic indicators exist for sexual orientation, substance addiction or even criminal inclination. Indeed due to continuous advances in science it is perhaps impossible to predict what information DNA may in the future reveal.

6. The fears of civil liberties groups are far from abstract and one has only to look at previous government initiatives in the area of eugenics across many countries, which have involved forced sterilisations, screening tests prohibiting marriage and the privacy issues that have arisen in many countries about HIV screening to see the type of issues such technologies can raise. DNA information also has a high commercial value as it is of interest to entities such as insurance companies and medical and pharmaceutical research and development companies.

A Human Rights Analysis

7. In looking at the human rights compatibility of the establishment of a DNA database, the ICCL uses a human rights analysis of what the implications of such a development would be. Such an analysis of any public policy is based on the approach by the European Court of Human Rights in examining potential human rights violations. The ICCL has considered:

- What is the nature of the proposal and does it raise *per se* human rights issues and potential interference with individual's rights?

- What is the purpose of the interference and is it a legitimate one?

- If it is a legitimate aim, is the interference *necessary* in a democratic society?

- In order to be necessary, is there a clear and evidentiary-based link between the measure and the aim?

- Does the measure strike a balance between the aim to be achieved and the protection of human rights, and is it non-discriminatory?

Why a DNA database?

8. It is very important in any discussion over the establishment of a DNA database to examine two separate issues:

- The use of DNA as a forensic tool in criminal investigation and prosecution and what specific purposes comprehensive DNA *retention* would serve.
- If a DNA database were to be set up what human rights issues does it raise and what protections are therefore necessary.

Use of DNA and practice in Ireland

9. In the context of criminal investigation, DNA is a very useful forensic means of establishing the presence of an individual at the scene of a crime, or the identity of an unidentified body. In the case of establishing a persons presence at a crime scene, by matching the DNA of a sample found at the crime of a scene to that of a suspect, it can establish that the suspect was present at the crime scene and could be used to rebut assertions that the suspect was not present. However, independently of any other corroborating information it can do no more than that. For example, in a case of rape, it can establish that a suspect had sexual relations with the victim, but can provide no evidence as to consent. DNA evidence can tell that a person was at a murder scene, but not independently why, when or if they had anything to do with the murder.

10. The use of DNA in this manner can be achieved by comparing the DNA profile of the sample at the crime scene against the DNA profile of any suspect in a crime. It is not necessary to have a DNA database to use DNA in such crime detection. In any criminal investigation, a comparison of the DNA profile to a list of suspects could be carried out. In the absence of consent a court order could be obtained seeking to take DNA samples, from any individual who could reasonably be a suspect. DNA has already been used in Ireland in several cases like this, without the need to resort to a DNA database.

11. DNA profiling was first used in a criminal case in Ireland in 1987 when a youth was convicted of the rape and murder of a 15-year-old woman, Carol Carpenter, in Tallaght. The convicted youth committed suicide in prison in 1994. Since 1994, profiling has been carried out at the Forensic Science Laboratory in Dublin, but samples are still sent to Britain where more sophisticated screening technology is used.

12. Under the Criminal Justice (Forensic Evidence) Act 1990, gardaí have the power to obtain blood, urine, saliva, dental imprints, footprints and swabs. Consent is required for blood, pubic hair, urine and saliva, which are deemed to be intimate samples. The Criminal Justice Bill 2003 proposes to reclassify saliva from being an intimate to a non-intimate body sample. Under the existing regime, all samples must be destroyed within six months, however under the Criminal Justice Bill, it is proposed to extend this to 12 months.

13. While until now there have been no moves to create a DNA database in Ireland, there has been some progress in compiling an Irish footprint databank (Sicar) used to detect individual shoe brands and to build up circumstantial evidence to link a criminal to a scene. Obviously, the

privacy issues of such a database are wholly different from those arising in the present context, but it is notable that we are not aware of any discussion of issues relating to the retention and destruction of samples that might arise in relation to Sicar.

What is a DNA Database

14. The current discussion relates to what is generally referred to as a Crime Sample Database. Such a database consists of a bank of samples obtained by a State agency or agencies through individuals' interaction with the criminal justice system. The retention of a body of samples is put forward as a means of quickly identifying offenders when DNA evidence is discovered at a crime scene. This relies on the sample bank of individual DNA profiles, including profiles of individuals who do not have an obvious connection with a particular crime scene and who are not suspects in that particular crime. It is based simply on the belief that early identification of suspects could occur from comparing crime scene DNA evidence with a collection of samples from persons who have previously otherwise been in contact with the criminal justice system.

15. The category of persons from whom samples are obtained and hence who comprise this database, can vary. It may be a narrow pool, for example convicted repeat sexual offenders, or a wider pool, for example all persons questioned by police in relation to any offence, or from anyone who has ever provided a DNA sample to police, whether voluntarily or involuntarily in the course of any investigation.

16. A DNA database can then be used in crimes where there is no suspect, to determine whether one of the individuals whose profiles are stored on the database could be matched to any sample taken from any crime site. A DNA database, as a crime detection tool, then only adds value in cases where there are DNA samples found at the scene of a crime and there are no suspects from whom DNA samples could be otherwise obtained. The absence of a DNA database does not prevent the use of DNA as a forensic tool. Paradoxically, it may be argued that the larger the database, the less efficacious it is likely to be in the quick detection of crime. Many jurisdictions where such systems already exist have witnessed dramatic expansions of the volume and range of categories of samples stored over time and questions have been raised as to whether the expansion of these databases have been managed with the aim of expediting law enforcement or as an end in itself.

Are there Human Rights Issues raised per se from the establishment of a DNA database?

17. There are a number of human rights issues, which arise from the use of a DNA database.

18. First issues arise from the taking of the DNA sample in the first place. Any procedure whereby samples – whether through saliva, hair or blood – are taken from an individual is, by its nature, intrusive and may raise issues of the bodily integrity of an individual. In situations where consent is present, the likelihood of issues of this arising are less, but in any case safeguards need to be in place to ensure that no danger of unlawful use of excessive force is used to obtain samples. These issues are further addressed at para. 34.

19. A second issue is one relating to privacy. The storing of DNA profiles, which can potentially reveal many personal details about the genetic characteristics of an individual, is an invasion of privacy *per se* and therefore needs to meet standards which will ensure the safeguarding of any further unlawful invasion of an individuals privacy.[1] The privacy issues which relate to the taking of samples include the regulation of the retention, storage and destruction of samples, and sharing of data.

20. A third issue is the interplay between the use of stored DNA profiles in the criminal justice system and the rights in particular of any accused to a fair trial. Amongst the concerns to be addressed here are the categories of persons from whom samples can be taken, the potential for mass screenings, access to DNA technology by both sides to a criminal charge – prosecution and defence, regulation of scientific expert witnesses, authenticity of data and vulnerability of data to theft or abuse and reliability of authentication technology.

21. A fourth concern is whether the DNA database will be open to use in a discriminatory matter – either in relation to the categories of profiles that are likely to be stored on it, its use in particular crimes, and the potential for genetic discrimination.

[1] E.g. *Rotaru v. Romania* [GC], no. 28341/95, §§ 43-44, ECHR 2000-V, *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, and *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 56, ECHR 2001-IX the Court has held that the recording of personal data – which could be information, your image e.g. on a CCTV camera or your voice - and the systematic or permanent nature of the record raises issues under Article 8.

Does a DNA database have a legitimate purpose?

22. The primary purpose for the establishment of a DNA database in this context is that of criminal investigation, although it could also have the potential to serve purposes of medical research. Alternatively other DNA databases set up for research purposes could be open to use by law enforcement agencies.[2] For the purposes of this analysis we will focus on DNA databases set up specifically for use in the criminal justice sphere. Such a purpose is of course a legitimate one recognised by human rights law. However it is important that the purpose is maintained and that there is no room allowed for the use of the database for any dual or secondary purpose i.e. that it is not subject to "function creep". In this regard we fully endorse the recommendation of the US National Research Council's Report on DNA Technology in Forensic Sciences that use of a database for other than law enforcement suspect identification purposes be expressly prohibited and subject to criminal penalties.

Is a DNA database necessary?

23. A DNA database is not necessary for the use of DNA in criminal investigations – DNA matching between suspects and DNA evidence samples, can be carried out in the normal course of an investigation. As indicated above, a

[2] In the UK there is controversy over the possible use by law enforcement agencies of a DNA database, set up to collect information on the lifestyle health and genes of 500,000 persons (BioBank Project). In the case of Stephen Kelly, police gained access to a medical study conducted at Edinburgh University, to determine his HIV status. See *The Independent*, 25 August 2003.

DNA database only becomes of specific use in the context of crimes where there are no suspects, but there is DNA evidence.

24. Given this specific use, in order to establish the necessity of a DNA database regard should be had to

- How many "no-suspect" unsolved crimes currently exist in Ireland which could possibly be assisted through a DNA database?
- In those "no-suspect" crimes is there reliable DNA evidence available from the crime scene?
- What is the rate in Ireland of "no-suspect" crimes, where the taking of DNA from suspects in the normal course of an investigation would not suffice to determine if there is a match to DNA samples from a crime scene?

We believe that before embarking on any efforts to establish a system of DNA retention, these basic evidential questions must be answered.

25. The establishment of a DNA database, irrespective of the framework in which it operates and the safeguards, will involve an increased infringement on individuals civil liberties as well as requiring significant state resources. The burden therefore lies with the state to prove that it is necessary in principle, and based on evidence, to adopt such a policy. It is not sufficient for the purpose to be one of administrative convenience.

26. We believe that in the absence of evidence that there is a sufficient volume of no-suspect crimes, in which DNA evidence could assist in the identification of suspects that the proposal for a DNA database should not be considered.

27. The volume of crime which a database could also potentially be of assistance in must also be balanced against the resource implications of such a database and whether it is an appropriate use of resources in light of the need to support other aspects of the criminal justice system. It is notable that in the UK, even before recent extensions of police powers to take DNA samples, the police had wide powers to take samples from all persons charged with or reported for a recordable crime. In practice, one of the principal reasons that this power was only exercised in relation to more serious cases was one of cost. A recent figure for testing of a sample in the UK was £40 sterling. Given that much of the testing of Irish samples is likely to continue to be carried out by UK laboratories, the cost element of establishing such a system here is likely to be significant.

28. In light of the limited resources available in the criminal justice sphere in Ireland, any decision to establish an Irish DNA database raises a wider issue of the efficacy and appropriateness of concentrating on DNA technology to the detriment of proper investigatory policing. DNA screening and the retention of a DNA database are extremely expensive initiatives. If the purpose of their use genuinely is crime detection and prevention then, serious issues arise as to whether the questionable crime reduction benefits justify the threat to individual liberties and the economic cost of such measures. In countries with the most extensive DNA database regimes, most notably the UK, there is strong evidence to suggest that the expansion of national

databases is the real objective of such policies, rather than a means by which crime reduction may be achieved.

29. Where there is evidence that the establishment of DNA database could be justified, then there are a number of other issues to be addressed to determine whether a balance would be achieved between its establishment, its potential benefits and the potential human rights violations that could occur.

The Framework of a DNA Database

30. In light of the privacy and fair trial issues which a DNA database raises, it is important to consider whether the establishment of such a database would be balanced against the civil liberties concerns that it raises.

Bodily Integrity

31. Roger Clark, a leading international authority in the area, has pointed out that as DNA technology concerns obtaining information not just about the person, but rather information of the person, intrinsic to them, this makes the very idea of such technology distasteful to people in many cultures, and of many religious persuasions. Under this technology persons have to submit to examination, that they may regard as demeaning.

32. In the case of taking DNA samples, which requires the person to provide a sample of body-fluid or body-tissue, this may be particularly acute. The invasive nature of taking samples should not be underestimated in terms of its potential to cause distress or humiliation, particularly where samples may be taken by force. In all cases, as a minimum the policy should be to adopt the least intrusive and least culturally offensive procedure. For example, if there is no scientific difference between obtaining DNA from a hair sample, and an oral swab, then the choice should be left to the suspect.

33. It is also vital that DNA samples should only be taken in the presence of a suspect's lawyer, even with consent. The taking of samples should also be video recorded with a copy of the recording made available to the person from

whom the sample is taken. We note that in the context of police interviews the European Committee on the Prevention of Torture has on three occasions called upon the government to change its policy on the right of a suspect to a lawyer during interrogation.[3]

34. Given the invasive nature of taking DNA samples, non-consensual testing should generally be strictly limited to persons convicted of serious offences. Any system of non-consensual testing for suspects should require judicial authorisation. As the DNA profile of a suspect cannot change over time, and the evidence if incriminating could be of central importance to a prosecution there is no reason why DNA evidence cannot be secured on foot of a court order, where any trier of fact based on the evidence can be confident of the legitimacy of the circumstances in which the evidence was obtained.

Privacy

35. The taking of DNA samples and then the subsequent recording and storing of DNA profiles raises issues of privacy *per se*. As well as the obvious dangers to privacy that spring from the taking of samples, more complex and far-reaching issues arise in relation to the retention and possible use of samples. As a basic point of principle, the consolidation of a wide range of personal data, including data as powerful as DNA samples in one State agency have a broad significance for the relation between the individual and the State. In essence, the central consolidation of this type of information greatly increases the opportunity for the State to exercise control over the population.

36. A key protection is the regulation of the retention of data prescribing that all samples be destroyed after a fixed period. This period should reflect the principle of proportionality and in line with general principles of data retention; all samples should be destroyed after a period of six months at the latest. It is also recalled that unlike for example a record of someone's telecommunications, DNA profiles of individuals can be recreated by taking a fresh sample from the individual if there is lawful reason to believe that it is necessary.

Information Sharing and Genetic Discrimination

37. Perhaps the greatest concern in relation to DNA retention is the unquestionable temptation to expand its usage. The maintenance of databases is highly expensive. Therefore to justify such costs, incentives arise to apply the potential of the database for multiple purposes.

38. Any multiple usage of identifiers represents a serious threat to privacy. There are no natural barriers to data-sharing and many countries lack laws to preclude it, and a strong tendency exists for organisations to break down such legal impediments as do exist. Hence the multiple purposes to which a database is applied can readily extend beyond a single state organisation to encompass multiple organisations in both the private and public sectors.

39. One of the key dangers posed by the extension of the use of DNA technology beyond the area of identification is that genetic information could be used by public or private agencies to discriminate against certain persons or groups. In the public sector, dangers arise in particular in relation to

[3] European Committee for the Prevention of Torture reports from 1993, 1998 and 2003 available at www.ecpt.coe.int.

the provision of services in the health sector. In the private sector, one example of genetic discrimination is where employers have discriminated against healthy employees on the basis of particular genetic characteristics of the employee which may or may not indicate higher risks for certain congenital conditions.

40. These examples highlight the need for safeguards and strict privacy and data protection structures to be put in place to ensure that whatever information is collected is confined to the criminal justice sphere. In this regard we would repeat our earlier recommendation that it would be an explicit offence for a databank to be used for any purpose other than that of identification of suspects in a criminal investigation.

Fairness in the Criminal Justice sphere

41. On the face of it, it might seem axiomatic that DNA technology should be as available to defendants as a means of exoneration as it is to prosecution authorities. However, in many jurisdictions, notably at the State level in the United States, such access is often severely restricted including the existence of bans on access for persons convicted of certain offences. For any retention system considered in Ireland it must be explicit that the results of DNA testing conducted by law enforcement agencies would be open to all parties as a means of exoneration as well as prosecution.

Mass Screenings

42. In August 2002, the Law and Justice Committee of the upper house of the New South Wales parliament recommended that judicial approval should be required before any mass DNA screenings were carried out. This recommendation was motivated in part by the concerns expressed by the NSW Privacy Commissioner that an overly wide definition of 'suspect' was being used to draw as many people as possible into the DNA testing 'net'. The Committee also expressed the concern that mass screenings constituted a wasteful use of police resources where good investigative practice could allow the police to carry out more targeted testing. In Australia, serious concerns had been expressed following a mass-screening operation during a murder investigation in a rural community at Wee Waa in NSW. In that case, police called upon 500 men from the town to surrender saliva samples however after several weeks it emerged that the perpetrator had, in fact, been one of the first suspects questioned and had confessed before the mass-screening had been conducted. The Government of NSW has since indicated that it will not act on the Committee's recommendations

43. In a recent murder investigation in Louisiana in the US, further concerns arose about the police concentration on carrying out a DNA dragnet, rather than focussing on credible evidence and suspicion. In that case, where a series of possibly linked murders was being investigated, eye-witness accounts was the basis for carrying out a DNA mass-screening of hundreds of white men. The ACLU expressed concern that eye-witness accounts are notoriously unreliable and this exercise might constitute a dangerous waste of police time and resources. Another serious concern related to evidence that police officers were exercising coercion on collecting 'voluntary' DNA samples.

44. In particular, there was evidence that, in cases where persons had refused to give samples on principle, officers had leaked their identities to the press and to the men's employers, in one case leading to the innocent man being suspended from work. There were many accounts of where police had implicitly or explicitly threatened people with a warrant or public disclosure of their identity if they failed to provide a sample. Similar problems were also reported in other mass-screenings in the US in recent years and this difficulty had also arisen in the Wee Waa investigation, where a lawyer who opposed the mass-screening suffered as a consequence.

45. The effectiveness of mass-screenings too is often overstated. In the UK, forensic science commentator Michael Strutt has pointed out that as UK police dedicate increasing proportions of their resources to DNA testing, crime rates remain static and clear-up rate is actually declining. He has called into question whether the real motivation for such testing is really crime detection at all, or is the aim more to increases the number of persons recorded in the UK's extensive national database. One of the most striking cases of mass-screening in the UK has been the investigation into the murder of Sara Cameron, where, despite the screening of 4,500 persons, no-one has yet been charged with the offence.

Reliability of Science

46. DNA evidence is essentially circumstantial in nature. It is a commonly misunderstood and misrepresented characteristic of DNA profiling that, unlike fingerprints, DNA sequences are not unique. Identification is based on comparing particular sections of two DNA samples and looking for differences, rather than comparing entire DNA sequences. By combining several such comparisons, the probability of a false match can then be reduced from one in several hundred to one in a million or even more. Even then, the possibility of a mismatch cannot be completely discounted and in the UK in 2000 evidence at the scene of a robbery was falsely matched to a sample on the existing national DNA database.

47. In general, the tighter the tolerances are set (to avoid false positives), the more false negatives will arise; and the looser the tolerances are set (to avoid false negatives), the more false positives occur. The tolerance is therefore set to reflect the interests of the scheme's primary sponsor, with little attention to the concerns of other stakeholders. It can be argued that DNA profiling does not carry the same danger of false negative testing as other biometric authentication methods (DNA profiles are not open to change over time as, say, hand or voice patterns might be).

48. In practice, measurements are seldom identical, and the comparison depends on the tolerance level that has been set for the application. This has the result that sometimes 'false positives' will occur, e.g. the assertion will be authenticated, even though the person who presented was not the one the system thought it was. On the opposite end of the spectrum, sometimes the right person will be rejected, in which are called 'false negatives' (e.g. they may have moved their finger at the wrong time, the part of the body used may be injured, or the behaviour being measured may have changed).

49. However unlikely a false match may be, the possibility of contaminated evidence or intentional manipulation of DNA samples cannot be discounted. More significantly, no technology can be immune from intentional contamination

Conclusions

1. The ICCL has serious reservations about the necessity of a DNA database to augment the already lawful use of DNA as a forensic tool in crime detection. Without evidence of a sufficient volume of crime, where specifically a DNA database, as oppose to the use of DNA testing, is essential, we do not believe that there is an appropriate public interest to warrant a measure which will both infringe on individual's civil liberties, and use a significant amount of limited state resources.

2. In the event that a DNA database proposal is considered the ICCL considers that the pool from which DNA samples should be collected should be narrow and limited to suspects of violent crime. In cases where consent for DNA samples is not given, then any enforced taking of DNA samples, should only be done under judicial supervision. Individuals should be advised of the purpose for which their DNA sample is being taken, what it can be used for and when it will be destroyed.

3. The retention period for such samples should also be strictly limited. In the cases of samples taken from suspects, who are not charged with any crime, or suspects who are acquitted of a crime the samples should be destroyed once the suspect is eliminated from police investigations. In the case where a suspect is convicted of a crime, the samples should be destroyed after a period of no more than six months. Individuals should be advised when their DNA profile is removed from the database.

4. In terms of control of the DNA database, strict safeguards must be put in place to ensure that the DNA profiles can only be used and accessed for the purpose of a specific Garda investigation into a crime for which there is DNA evidence available. DNA profiles stored on a database must not be used for any secondary purpose.

5. Mass screenings of individuals in the investigation of a crime must not be carried out.

Annex I
Comparative Analysis

US

The US system has gone from only taking samples from convicted sex offenders to taking from persons arrested and not convicted of a crime. The ACLU has argued for regulation of CODIS (the Combined Offender DNA Index System) so that only persons convicted of serious violent felonies should have their DNA entered into CODIS, that defendants should have access to CODIS to prove their innocence and that all samples used to provide DNA should be destroyed. In several states, convicted persons are currently not allowed access to DNA evidence that might exonerate them.

UK

The UK has the most extensive regime of DNA collection and retention of any EU State. In 2000 it was estimated that 500,000 samples were in the national DNA database. While originally, samples were only taken from a narrow group of convicted offenders, currently police are empowered to take samples from anyone suspected of, charged with, or reported for a recordable crime. Cost implications have meant that in practice it is only in relation to serious crime that a police chief constables to direct the taking of samples. If a person is not prosecuted or is acquitted, their samples must be destroyed.

However, there have been proposals to retain the samples of anyone who has given a sample voluntarily. This would have an important impact on "mass-screenings" during serious crime investigations where large populations voluntarily donate samples on the basis that these samples will be destroyed afterwards. On one level, it may discourage people from volunteering samples, while also potential creating the suspicion that anyone who does not volunteer a sample is a suspect in the investigation.

In June 2000, a three month pilot scheme was put in place to add the DNA profiles of all drug offenders to the National DNA Database. There is also provision in UK law for police to take DNA samples by force. Similar provisions in the US in relation to persons detained in prisons have been found unconstitutional. The UK Police Superintendents Association has gone as far as to call for all children to be profiled at birth.

EU

A 1997 EU Council Resolution on the exchange of DNA analysis results called on member states to establish national databases with standardised technology. A European DNA Profiling Group has existed since 1988 with the aim of "informally pursuing the aim of exchanging DNA profiles". In 1998 an agreement was reached within the European Network of Forensic Science Institutes DNA Working Group on the harmonised use of DNA markers in the member states.