CONFLICTING BILLS: DNA V. PDP

by

Professor Abu Bakar Munir* & Teh Tai Yong **

MALAYSIA

Introduction

The Deoxyribonucleic Acid Identification Bill 2008 ("DNA Bill") was first read in the *Dewan Rakyat*[1] on 18 August 2008. The tabling of the DNA Bill in the *Dewan Rakyat* has caused much controversy surrounding its provisions, timing, speed and the purpose of introducing the bill. There are a few draconian provisions in the DNA Bill which caught the attention of the lawmakers and the same have been vigorously debated in Parliament in August 2008. Amongst the matters raised by the MPs during the debate in Parliament were that the Data Protection Act should be passed and implemented first before the DNA Bill, the manner in which a non-intimate sample could be taken from an individual and the effect of refusal for giving the non-intimate sample, the conclusiveness of the information from the DNA databank, etc.[2]

This paper examines the issues relating to the DNA Bill from the perspective of data protection principles. The aim is to dissect the implications and/or conflicts between the DNA Bill and the data protection principles. The paper makes a comparative analysis with the DNA Bill from other jurisdictions such as the United Kingdom, Australia, Canada and Trinidad & Tobago.

For the purposes of discussion in this paper, the data protection principles as stated in the proposed draft of the Personal Data Protection Bill ("PDP Bill") circulated by the then Ministry of Energy, Communications and Multimedia (now the Ministry of Energy, Water and Communications) in 2000 are used as reference.[3]

What Is DNA & Is DNA Personal Data?

Deoxyribonucleic acid (DNA) is a nucleic acid that contains the genetic instructions used in the development and functioning of all known living organisms[4] DNA, found in virtually every cell in the body, contains genetic information that helps determine physical characteristics. A person's DNA is unique with the exception of identical twins. An individual inherits half their DNA from their father and half from their mother. Closely related individuals such as siblings have more similarities in their DNA than unrelated individuals. DNA profiling examines discrete parts of an individual's DNA that vary greatly from one person to another.[5]

Section 2(1) of the PDP Bill defines "personal data to mean "any information recorded in a document in which it can practically be processed wholly or partly by any automatic

means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user, including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual."

From the definition above, DNA obviously is personal data as it relates directly to a living individual who is identified or identifiable from the analysis of DNA profiles. The probability of matching DNA profiles of two persons not related to each other is less than 1 in 1 billion. That would mean that accuracy of identifying a person through DNA is more than 99.99%. DNA is widely used by law enforcement agencies around the world. Such a breakthrough in technology has changed the landscape of crime-fighting as DNA serves as a powerful tool in identification of the criminals.

Undoubtedly, there are tremendous benefits in using DNA as a crime-fighting tool. Many countries such as the United Kingdom and the United States have enacted legislation to establish the DNA databank and empower the law enforcement agencies to collect, process and store DNA of individuals.

However, as it involves collecting, processing and storing of personal data, it is equally important that the data protection principles are adhered to by the law enforcement agencies. Lawmakers of the countries having DNA legislation should also enact data protection laws to ensure that data protection principles are complied with by the law enforcement agencies. The United States and many European countries have taken the path of enacting data protection laws. This would serve as a check and balance against the powers granted to agencies and/or officers dealing with DNA.

It is opined, therefore, that the Malaysian Parliament should also consider such aspects before passing the DNA Bill. The benefits of DNA as a tool in combating crime are well recognised and undisputed. But the personal data to be collected, processed and stored in the DNA databank must be dealt with in accordance with data protection principles.

Application Of The Data Protection Principles To DNA Bill

The operation of the DNA Databank is entrusted upon the Head, Deputy Head and officers of the DNA Databank, who are appointed by the minister charged with the responsibility of internal security (in the present context, the Home Minister), pursuant to s. 7 of the DNA Bill.

Section 7(1) of the DNA Bill provides that the Minister shall appoint a police officer not below the rank of Deputy Commissioner of Police as Head of the Forensic DNA Databank, whilst s. 7(2) of the DNA Bill provides that the Minister shall appoint a police officer not below the rank of Senior Assistant Commissioner of Police as Deputy Head of DNA Databank. It is noted that the top positions of the DNA Databank are to be held by police officers.

Section 18 of the Police Act 1967[6] ("PA") states that every police officer shall unless expressly excluded be subject to the same provisions as are applicable to other public officers of corresponding status in the service of the Government of Malaysia. Further, s. 4 of the PA states that the Royal Malaysian Police Force shall be under control of an Inspector-General who shall be responsible to the Minister for the control and direction of the Force. That would mean that if the PDP Bill applies to the Government, the police acting as the top officers of DNA Databank must comply with the data protection principles.

The PDP law ought to apply to the Government. The Government possesses massive amount of personal data. The amount of personal information the Government holds and processes is equal, if not more, than the private sector. Without such legislation, there is a possibility of misuse if the personal data fell into the hands of unscrupulous parties. The implications of abuse and mismanagement of personal data in the public sector have been acknowledged by many countries.

If the issue of data protection in the Government sector is not properly regulated, it could result in great abuse and wide surveillance over the citizen beyond the powers of the agencies. Gordon Hughes argued that any legislative purpose to the issues involved in computerised information storage would be incomplete if only the public or only the private sector is regulated.[7]

A similar view was also stated in the White Paper (United Kingdom) "Computers and Privacy"[8] in 1975 which read "Much of the information now going into (government) computers because it is eminently suitable for processing by computer is regarded by most people as particularly sensitive: medical records, financial information and so on. The public is, therefore, entitled to have satisfactory assurances that its data and especially those which are sensitive are held and used responsibly, with due regard to accuracy, completeness, relevance, security and confidentiality."

The EU Data Protection Directive 1995[9], the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data 1980, the Canadian Privacy Act 1982, the Australian Privacy Act 1988, the United Kingdom Data Protection Act 1998 and the Hong Kong Personal Data (Privacy) Ordinance have all taken the approach that the public sector and the government in those jurisdictions are subject to the data protection laws.

The PDP Bill ought to be applied to the public sector and the Government, even if it is not expressly provided. Section 13 of the Interpretation Acts 1948 and 1967[10] ("IA") states that "Every Act shall be a public Act unless the contrary is expressly provided therein." Section 17A of the IA states that "In the interpretation of a provision of an Act, a construction that would promote the purpose or object underlying the Act (whether that purpose or object is expressly stated in the Act or not) shall be preferred to a construction that would not promote that purpose or object." The preferred approach would be to include the Government in order to "regulate the protection of personal data relating to individuals" as provided in the preamble of the PDP Bill.

Based on the above, it is argued that the Head, Deputy Head and officers of the DNA Databank shall comply with the data protection principles. Of course, the compliance of the data protection principles is subject to the enactment of the data protection laws before the passing of the DNA Bill. Hence, it is pertinent to enact the data protection laws first in order to ensure that the data protection principles are complied with by the DNA Databank. Or else, efforts must be made to ensure that the DNA Bill complies with the data protection principles and other relevant provisions of the data protection law.

Compliance With The Data Protection Principles

Principle 1 - Manner Of Collection Of Personal Data

The first principle states that personal data shall be collected fairly and lawfully. It should be noted that as long as the DNA Bill authorises a certain manner of collection of DNA samples from individuals, the manner of collection of the personal data is lawful, as it is prescribed by law. However, the real issue is whether the personal data is collected fairly.

The DNA Bill makes a distinction between taking of an intimate sample[11] and taking of a non-intimate sample.[12] Intimate sample is defined to mean "(a) a sample of blood, semen or any other tissue or fluid taken from a person's body, urine or pubic hair; or (b) a swab taken from any part of a person's genitals (including pubic hair) or from a person's body orifice other than the mouth" whereas non-intimate sample is defined to mean "(a) a sample of hair other than the pubic hair; (b) a sample taken from a nail or from under a nail; (c) a swab taken from any part of a person's body other than a part from which a swab taken would be an intimate sample; or (d) saliva".[13]

Appropriate Consent (Intimate Sample)

Taking of an intimate sample requires "appropriate consent" in the prescribed form is given by the person from whom an intimate sample is to be taken.[14] Appropriate consent is defined to mean (a) in relation to a person who is under the age of eighteen years, the consent in writing of his parent or guardian; (b) in relation to a person who has attained the age of eighteen years, the consent in writing of that person; or (c) in relation to a person in whom there is a condition of arrested or incomplete development of mind or body whether such condition arises from inherent causes or is induced by disease or injury and who is incapable of understanding the general nature and effect of a forensic DNA analysis or is incapable of indicating whether he consents or does not consent to give his intimate sample or non-intimate sample, the consent in writing of his parent or guardian.[15]

It would be interesting to refer to the position in Trinidad & Tobago. Section 14(4) of the Deoxyribonucleic Acid (DNA) Act 2007 provides that "Where an authorization is given and it is proposed that an intimate sample shall be taken in pursuance of the authorization, a police officer shall seek the consent of the suspect and before he gives his consent the police officer shall:

(a) show him a copy of the authorization and where necessary read it to him;

(b) inform him that if he consents, the sample may be the subject of a search;

(c) advise that if he does not respond within a period of two hours after the request is made, he is deemed to have refused to consent to the taking of the sample;

(d) inform him of his right to withdraw his consent before the sample is taken;

(e) inform him that he has the right to consult with and have present an attorney-at-law, or an adult of his choice, before consenting to the taking of the intimate sample; and

(f) inform him that he may waive his right under paragraph (e), in the form set out as Form 4 in the First Schedule, in the presence of an officer of the First Division.

Under the DNA Bill, if a person or his/her parent or guardian (as the case may be) refuses to give consent, no intimate sample could be taken from the person. However, ss. 19 and 20 of Trinidad & Tobago Deoxyribonucleic Acid (DNA) Act 2007 provide for the procedure of obtaining intimate sample by order of court as follows:

19(1) Where a suspect refuses to consent to give an intimate sample, an investigating officer may make an application to the court for an order directing that an intimate sample be taken without his consent.

...

20(1) Where an application is made under section 19, the applicant shall satisfy the court that on the evidence before it there are reasonable grounds to believe that the:

(a) person against whom the Order is sought is associated with the commission of or committed an offence;

(b) intimate sample sought to be taken is likely to produce evidence tending to confirm or disprove that that person was associated with the commission of or committed an offence; and

(c) taking of the intimate sample is justified in all the circumstances.

20(2) In determining whether an order is justified in all the circumstances, the court shall balance the public interest of obtaining DNA evidence from an intimate sample against the public interest of upholding the physical integrity of the individual.

20(3) In balancing those interests, the court shall consider the following matters:

(a) the circumstances surrounding the commission of the offence and the gravity of the offence;

(b) the degree of the person's alleged participation in the commission of the offence;

(c) the age, physical health and mental health of the person;

(d) if the person is a child or an incapable person, the welfare of that person;

(e) whether there is a less intrusive but reasonably practicable way of obtaining evidence tending to confirm or disprove that the person was associated with the commission of or committed the offence;

(f) the reason, if any, for refusing to consent;

(g) whether there is a report in relation to a non-intimate or an intimate sample; and

(h) any other matter considered relevant to balancing those interests.

The provision to apply for a court order if a person refuses to give a sample is also provided for in the laws relating to DNA in Australia. Section 464T of the Crimes Act 1958 provides that:

(1) If:

(a) a person refuses to undergo a forensic procedure after being requested to do so or is incapable of giving informed consent by reason of mental impairment; and

(b) the sample or examination sought may be obtained by a compulsory procedure; and

(c) the person is a relevant suspect; and

(d) a member of the police force believes on reasonable grounds that the person has committed the offence in respect of which the procedure was requested:

the member may apply to the Magistrates' Court for an order directing the person to undergo the compulsory procedure.

The court may make an order directing a person to undergo a compulsory procedure if the court is satisfied on the balance of probabilities that the person is a relevant suspect; there are reasonable grounds to believe that the person has committed the offence in respect of which the application is made; there are reasonable grounds to believe that the conduct of the procedure on the person may tend to confirm or disprove his or her involvement in the commission of the offence; the person has refused to give consent to a request or the person is incapable of giving informed consent by reason of mental impairment; in all the circumstances, the making of the order is justified etc.

Crucially important is the insertion of sections relating to procedure of obtaining an intimate sample by order of court in the DNA Bill. It does not erode the rights of the

person whom the intimate sample is to be taken as there are conditions that have to be satisfied before the court will grant such order. Wisely, this is the preferred approach compared to obtaining the sample by use of *all means necessary* pursuant to s. 13(7) of the DNA Bill as would be discussed later.

Appropriate Consent (Non-intimate Sample)

The procedure of taking non-intimate samples is more draconian. In contrast to taking of an intimate sample, appropriate consent is not required for a non-intimate sample to be taken from a person. There is no corresponding provision for s. 12(2)(B) of the DNA Bill (which requires appropriate consent of a person for taking of an intimate sample) under s. 13 relating to taking of a non-intimate sample. That would mean a non-intimate sample could be taken from a person with or without his or her consent, subject to the authorization under s. 13(3) of the DNA Bill by the authorised officer.

In the United Kingdom, s. 10 of the Criminal Justice Act 2003 amending s. 63 of the Police and Criminal Evidence Act 1984 states that a non-intimate sample may be taken from a person without the appropriate consent if two conditions are satisfied. Firstly, the person is in police detention in consequence of his arrest for a recordable offence. Secondly, he has not had a non-intimate sample of the same type and from the same part of the body taken in the course of the investigation of the offence by the police, or he has had such a sample taken but it proved insufficient.

Section 464SA of the Australian Crimes Act 1958 provides for the police officer to authorise non-intimate compulsory procedure. A senior police officer who is not involved in investigating the offence for which the compulsory procedure is required may authorise the conduct of a non-intimate compulsory procedure on a person if the senior police officer is satisfied that the person is a relevant suspect; the person is not under the age of eighteen years; the person is not incapable of giving informed consent by reason of mental impairment; the person has refused to give consent to a request; there are reasonable grounds to believe that the person has committed the offence in respect of which the authorisation is sought; in all the circumstances, the giving of the authorisation is justified etc. Under s. 464B of the Crimes Act 1958, before a senior police officer gives or refuses to give an authorisation under s. 464SA, the senior police officer must allow the suspect or the suspect's legal practitioner, if any, a reasonable opportunity, if practicable in person, to inform the senior police officer whether there is any reason why the non-intimate compulsory procedure should not be conducted.

In Trinidad & Tobago, s. 5 of the Deoxyribonucleic Acid (DNA) Act 2007 states that "a non-intimate sample may be taken from a person without his consent where (a) he has been charged with an offence; (b) a stain derived from a crime scene exists and there are reasonable grounds for suspecting that that person was involved in the offence and for believing that forensic DNA analysis could confirm or disprove such suspicion; (c) he has had a non-intimate sample taken and that sample has proved to be either unsuitable or insufficient for forensic DNA analysis; or (d) he has been convicted of an offence and is serving a term of imprisonment.

Pursuant to s. 7 of Trinidad & Tobago Deoxyribonucleic Acid (DNA) Act 2007, although the consent is not required to take a non-intimate sample, a police officer shall *notify* the person in writing from whom a non-intimate sample is to be taken under s. 5(a), (b) and (c) of the reason for taking a sample and that his DNA profile may be the subject of a search.

This is in line with the first data protection principle which also provides that where personal data are to be collected from a data subject, all practicable steps shall be taken to ensure that the data subject is explicitly informed whether it is obligatory or voluntary for him to supply the personal data (if obligatory, the consequences for failing to supply the personal data); the purpose of collection; his right to access and to request correction; and the class of persons to whom the personal data may be transferred.

The safeguards, as provided for in other jurisdictions, are non-existent in the DNA Bill. The Bill must provide some safeguards for the taking of a non-intimate sample.

Authorised Officer And Persons Taking The Sample

Under the DNA Bill, an authorised officer shall only give his authorization to take an intimate sample or a non-intimate sample (as the case may be) of a person under certain limited situations stated in ss. 12(3) and 13(3), namely (a) he has reasonable grounds for (i) suspecting that the person from whom the intimate sample or non-intimate sample (as the case may be) is to be taken has committed an offence; and (ii) believing that the sample will tend to confirm or disprove the commission of the offence by that person; (b) an arrest has been effected on or a detention order has been made against a detainee under any law made pursuant to arts. 149 or 150 of the Federal Constitution; or (c) an order or a decision has been made pursuant to the Drug Dependants (Treatment and Rehabilitation) Act 1983 against a drug dependant.

It should be noted that the word "offence" is defined very widely under s. 2 of the DNA Bill, ie, "*any act or omission punishableby any law* for the time being in force", which is in contrast with the position in Canada (where it applies to certain designated offence within the meaning of s. 487.04 of the Criminal Code or s. 196.11 of the National Defence Act).[16] The DNA Bill gives the authorized officer wide powers to authorize the taking of a DNA sample from any person for any act or omission punishable by any law for the time being in force.

An authorised officer is defined under s. 2 of the DNA Bill to mean any police officer not below the rank of Deputy Superintendent of Police. It is opined that if such Bill is passed, the rank of Deputy Superintendent of Police as *authorised officer* must be maintained and should not be amended to police officers ranked lower than Deputy Superintendent.

This is seen in the United Kingdom Criminal Justice and Police Act 2001, amending ss. 62 and 63 of the Police and Criminal Evidence Act 1984, which has lowered the required rank of an authorized officer (for the purpose of taking intimate and non-intimate samples) from superintendent to inspector. In Australia, the authorizing officer under s.

464SA of the Crimes Act 1958 is "senior police officer", which is defined to be a police of or above the rank of senior sergeant.[17]

Under the DNA Bill, an intimate sample shall only be taken by a government medical officer.[18] A non-intimate sample could be taken by government medical officer, a police or a chemist.[19] It is opined that an intimate or non-intimate sample could be taken by a medical officer (regardless of whether he or she is from the government or private sector) provided the standard procedures are strictly adhered to by the medical officer. Distinction should not be made between medical officers practising in the government or private sector.

The filter or point of control should be the procedural aspect ie, whether standard procedures are strictly adhered to by the medical officer and not whether the medical officer is practising in the government or private sector. Reference is made to the position in Australia, which states that "A sample must be taken or a physical examination must be conducted if taken or conducted by a medical practitioner, nurse or dentist, in a *manner consistent with the appropriate medical or dental standards*."[20]

Use Of All Means Necessary & Criminalising Refusal To Give Sample

A police officer may use *all means necessary* for the purpose of taking or assisting the taking of a non-intimate sample from a person, pursuant to s. 13(7) of the DNA Bill. The means necessary for taking the sample is not subject to the test of reasonableness. As long as a police officer thinks that it is necessary, he or she is allowed to deploy *all means necessary* to take or assist to take the non-intimate sample from a person.

In addition, the DNA Bill criminalises the refusal to give non-intimate sample by a person. Section 14 of the DNA Bill states that:

If a person from whom a non-intimate sample is to be taken under this Act:

(a) refuses to give such sample;

(b) refuses to allow such sample to be taken from him; or

(c) obstructs the taking of such sample from him,

commits an offence and shall, on conviction, be liable to a fine not exceeding ten thousand ringgit or to imprisonment for a term not exceeding one year or to both.

There is a drafting error in the section as it does not state *who* commits the offence. It should instead read as:

If a person from whom a non-intimate sample is to be taken under this Act -

(a) refuses to give such sample;

(b) refuses to allow such sample to be taken from him; or

(c) obstructs the taking of such sample from him,

that person commits an offence and shall, on conviction, be liable to a fine not exceeding ten thousand ringgit or to imprisonment for a term not exceeding one year or to both.

There are several objections to s. 14 of the DNA Bill. Firstly, such criminalising section is unfair and non-existent in the legislation of other jurisdictions. Refusal to give a sample could lead to an adverse/negative inference when an accused is charged in the court, but it should not be criminalised.[21] Secondly, such section may lead to an accused person deliberately refusing to give a sample if the offence being heard by the court carries a much higher sentence. For example, an accused for murder would rather refuse to give a sample and elect to be fined ten thousand ringgit and/or jailed for one year. Thirdly, the police may exercise the wide powers given pursuant to s. 13(7) of the DNA Bill discussed above. It would not be unreasonable to imagine that the police would be able to take the sample when *all necessary means* are deployed to do so.

Hence, it is suggested that s. 14 of the DNA Bill ought to be deleted. A provision to obtain a court order, as discussed above, should be inserted instead. If a person refuses to give a sample, an application could be made to the court for an order to take sample rather than resorting to *use of all means necessary bypolice*[22] and *criminalising the act of refusal*.[23]

Principle 2 - Purpose Of Collection Of Personal Data

The second principle states that personal data shall be held for one or more specified and lawful purposes. Personal data shall not be collected unless the personal data is collected for a specified lawful purpose or directly related to the purpose and such personal data is necessary, adequate, relevant but not excessive in relation to that purpose.

In order to discuss the specified purposes in the DNA Bill, reference is made to s. 4 (Objectives of the DNA Databank), which made reference to the indices to be established under the DNA Databank under s. 3(3) of the DNA Bill. Section 4 of the DNA Bill states that:

(1) The primary objective of the DNA Databank is to keep and maintain the *indices referred to in subsection 3(3)* for the purpose of human identification in relation to forensic investigation.

(2) In addition to subsection (1), the DNA profiles and any information in relation thereto kept and maintained in the DNA Databank may be used in assisting - (a) the recovery or identification of human remains from a disaster or for humanitarian purposes; and (b) the identification of living or deceased persons.

Arguably, the indices established under s. 3(3) of the DNA Bill are extremely wide. The seven indices under the DNA Databank under the management, control and supervision of the Head of DNA Bank are as follows:

(a) a crime scene index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample that is found -

(i) on any thing or at any place where an offence was committed;

(ii) on or within the body of a victim of an offence;

(iii) on any thing worn or carried by the victim of an offence at the time when the offence was committed; or

(iv) on or within the body of any person reasonably suspected of having committed an offence;

(b) a suspected persons index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample taken from persons reasonably suspected of having committed an offence and includes suspects who have not been charged in any court for any offence;

(c) a convicted offenders index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample taken from persons convicted of any offence under any written law;

(d) a detainee index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample taken from a detainee;

(e) a drug dependants index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample taken from a drug dependant;

(f) a missing persons index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample taken from -

(i) the body or parts of the body of an unidentified deceased person;

(ii) any thing worn or carried by a missing person; or

(iii) the next of kin of a missing person if so required; and

(g) a voluntary index which shall contain DNA profiles and any information in relation thereto derived from an intimate sample or a non-intimate sample taken from a person who volunteers to submit the same for the purpose of storage of the DNA information in the DNA Databank and for such other purposes referred to in paragraph 15(2)(a).

Such wide indices to be established under the DNA Databank gives the data user wide powers to collect personal data for the purposes and directly related purposes specified therein. Comparison is made with the position in Canada where its DNA databank only consists of two indices, namely the crime scene index and convicted offenders index stated in s. 5 of the Canadian DNA Identification Act 1998. This is consistent with the purpose stated in s. 3 of the Canadian DNA Identification Act 1998, ie, to establish a national DNA databank to help law enforcement agencies in identifying persons alleged to have committed designated offences.

In contrast, Australia has a wide DNA database system under s. 464 of the Crimes Act 1958, which includes crime scene index; missing persons index; unknown deceased persons index; serious offenders index; volunteers (unlimited and limited purposes) index; suspects index; statistical index; and any other prescribed index.

We are of the view that the position in Canada is the preferred one as the following principles are expressly provided in s. 4 of the Canadian DNA Identification Act 1998:

It is recognised and declared that:

(a) the protection of society and the administration of justice are well served by the early detection, arrest and conviction of offenders, which can be facilitated by the use of DNA profiles;

(b) the DNA profiles, as well as samples of bodily substances from which the profiles are derived, may be *used only for law enforcement purposes in accordance with this Act, and not for any unauthorized purpose;* and

(c) *to protect the privacy of individuals with respect to personal information* about themselves, *safeguards* must be placed on

(i) the use and communication of, and access to, DNA profiles and other information contained in the national DNA data bank, and

(ii) the use of, and access to, bodily substances that are transmitted to the Commissioner for the purposes of this Act.

Recognition is expressly given to the *privacy of individuals with respect to personal information* as stated above. Proper safeguards must also be put in place in order to protect the privacy of individuals. The DNA Bill should also adopt such an approach. Once proper safeguards are provided for the use, communication and access of the personal data, many would feel more comfortable with such a law and the reservations on implementation of this law may be minimised or eliminated.

Principle 3 - Use Of Personal Data

The third principle states that personal data held for any purpose shall not, without the consent of the data subject, be used for any purpose other than the purpose or directly related purpose for which the personal data was to be used at the time of collection.

Section 20(1) of the DNA Bill states that:

No person who receives a DNA profile for entry in the DNA Databank or who has access to information contained in the DNA Databank shall, except in accordance with sections 11 and 23, *use or communicate* such DNA profile or any information in relation thereto to be used or communicated other than for the *purpose* of this Act.

Any person who contravenes s. 20(1) of the DNA Bill above commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding five years or to a fine not exceeding fifty thousand ringgit or to both.[24]

As stated above, one of the exceptions is provided under s. 11 of the DNA Bill. It provides that "The access to, a communication or use of DNA profiles and any information in relation thereto stored in the DNA Databank by the Head of DNA Databank, Deputy Head of DNA Databank, DNA Databank officers and any chemist shall only be for the purposes of - (a) forensic comparison with any other DNA profiles or information in the course of an investigation of *any offence* conducted by *any enforcement agency*; (b) administering the DNA Databank; or (c) making the information available to the person to whom the information relates.

The matter of concern here relates to the *wide purpose* under s. 4 (which referred to s. 3) of the DNA Bill as discussed above. The data user may use the personal data for a purpose (which is already wide) or for a directly related purpose. Moreover, the data user may use the DNA profiles for forensic comparison in the course of an investigation of *any offence* (which is given its widest meaning).

Contrastingly, the information on a DNA database in Australia may only be used for forensic comparison permitted under s. 464ZGI of the Crimes Act 1958 (permissible matching). Similarly, in Canada, the Commissioner shall conduct a forensic DNA analysis of the bodily substances transmitted if satisfied that the offence referred to in the order or authorisation is a *designated offence*, pursuant to s. 5.1(2) of the Canadian DNA Identification Act 1998.

Further, forensic comparison could be done in the course of investigation of any offence by *any enforcement agency*. The phrase "enforcement agency" is not defined in the DNA Bill. But the word "any" appearing before the phrase would give a wide meaning to "enforcement agency". Given its widest interpretation, "enforcement agency" may include the police force, anti-corruption agency, customs and immigration force, local authority etc. It is pertinent that data protection laws (PDP Bill) apply to all these organisations (whether in the public or private sector) in order to effectively protect the privacy of individuals in relation to personal data.

As for foreign law enforcement agencies, the Head of DNA Databank may, upon request by a foreign law enforcement agency, compare a DNA profile received from the foreign law enforcement agency with the DNA profiles in the DNA Databank in order to determine whether such DNA profile is already contained in the DNA Databank and communicate any relevant information to the foreign law enforcement agency, pursuant to s. 23 of the DNA Bill. It is equally important for the PDP Bill to adopt the "adequate level of protection" principle for a transborder flow of personal data to other countries similar to art. 25 EU Data Protection Directive 1995. This is to ensure that the personal data is granted adequate levels of protection when it is transmitted to a foreign law enforcement agency.

In order to have effective cooperation with foreign law enforcement agencies, there is a need to enact data protection laws (by passing the PDP Bill) because many countries already have data protection laws in place and the "adequate level of protection" principle is entrenched in it, for example Principle 8 as stated in Schedule 1 of the United Kingdom Data Protection Act 1998. There is a risk for foreign law enforcement agencies to refuse to cooperate because of the lack of or non-existence of data protection if the PDP is not enacted.

Principle 4 - Disclosure Of Personal Data

The fourth principle states that personal data shall not, without consent of the data subject be disclosed unless the disclosure is done for the purpose or is directly related to the purpose in connection with which the personal data was obtained.

As discussed above, s. 20 of the DNA Bill prohibits the unauthorised use and communication of DNA profiles or information. This is coupled with s. 21 of the DNA Bill which states that:

The Head of DNA Databank, Deputy Head of DNA Databank and DNA Databank officers or any person who for any reason, has by any means access to any data, record, book, register, correspondence, document whatsoever, or material or information, relating to the DNA profiles and any information in relation thereto in the DNA Databank *which he has acquired in the performance of his functions or the exercise of his powers*, shall not give, divulge, reveal, publish or otherwise disclose to any person, such document, material or information unless the disclosure is required or authorized -

(a) under this Act or regulations made under this Act;

(b) under any written law;

(c) by any court; or

(d) for the performance of his functions or the exercise of his powers under this Act or regulations made under this Act.

This is a fine provision to ensure secrecy of the personal data. Any person who contravenes the secrecy provision above commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding five years or to a fine not exceeding fifty thousand ringgit or to both.[25]

However, s. 21 of the DNA Bill does not cover the "outsiders" other than the specified officers. For example, the tea lady who works in the DNA Databank who accidentally comes across a DNA profile or the thief who stole a DNA profile from the DNA Databank. Although s. 21 includes any person who *for any reason, has by any means access to any data, record, book, register, correspondence, document whatsoever, or material or information, relating to the DNA profiles and any information in relation thereto in the DNA Databank* (which includes the "outsiders"), but this is qualified by the subsequent sentence *"which he has acquired in the performance of his functions or the exercise of his powers".* Outsiders such as the tea lady or thief mentioned above do not *legally and properly* acquire the information *in the performance of his/her functions or the exercise of his/her powers,* hence they are not subject to the said provision. Therefore, the qualification *(which he has acquired in the performance of his functions or the exercise of his powers)* should be deleted from s. 21 of the DNA Bill.

In this respect, reference is made to the provision in s. 6(7) of the Canadian DNA Identification Act 1998, which states, "Subject to this section, *no person* shall communicate any information that is contained in the DNA data bank or allow the information to be communicated." Further, s. 50(1)(c) of the Trinidad & Tobago Deoxyribonucleic Acid (DNA) Act 2007 states that "*A person* who wilfully and without authorization - discloses or obtains DNA data or DNA profiles, commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars and to imprisonment for seven years." A similar approach is adopted by Australia wherein s. 464ZGK of the Crimes Act 1958 states that *a person* who intentionally or recklessly causes the disclosure of information other than as provided by this section is guilty of an offence. This would include *any person,* namely the designated officers in the DNA databank and the "outsiders".

Principle 5 - Accuracy Of The Personal Data

The fifth principle states that all practicable steps shall be taken to ensure that personal data is accurate, complete, relevant, not misleading and up-to-date, having regard to the purposes (including any directly related purpose) for which the personal data is, or is to be, used.

Section 9(1) of the DNA Bill states that "The Head of DNA Databank *shall be entitled* to rectify the particulars in the DNA profiles and any information in relation thereto if - (a) a clerical error has occurred; and (b) sufficient evidence is produced to satisfy him that the entry made is incorrect, and on making the rectification he shall, where necessary, issue to the person entitled to the information derived from the analysis of the sample taken for him, the particulars so rectified." The powers of rectification under this section shall be

exercised by the Head of DNA Databank alone in accordance with s. 9(2) of the DNA Bill.

In addition, ss. 19 and 22 of the DNA Bill provide for the offence of tampering, abetting or attempting to tamper with samples, DNA profiles and information. Contravention to these sections is punishable by imprisonment for a term not exceeding five years or to a fine not exceeding fifty thousand ringgit or to both for the offence of tampering with samples, DNA profiles and information; or imprisonment for a term not exceeding two and half years or to a fine not exceeding fifty thousand ringgit or to both for the offence of abetting or attempting to tamper with samples, DNA profiles and information.

These are commendable provisions to ensure that the personal data on DNA Databank is accurate. However, before the DNA profile and/or any information in relation thereto are rectified by the Head of DNA Databank, the information from the DNA Databank is admissible as conclusive proof in any proceedings in any court as provided under s. 24 of the DNA Bill. Section 24 is probably one of the most controversial sections in the DNA Bill. It provides that:

Notwithstanding any written law to the contrary, any information from the DNA Databank shall be admissible as *conclusive proof* of the DNA identification in any proceedings in any court.

The fact that s. 9 (which allows the Head of the DNA Databank to rectify any particulars of the DNA profile or any information in relation thereto) is inserted in the DNA Bill would mean that there is a possibility of having an error in the DNA profiles and/or any information in relation thereto. Such error could either be deliberate or accidental in nature. Even if the DNA profiles and/or any information in relation thereto are not rectified by the Head of DNA Databank, they should be capable of being challenged though proceedings in court. The judges, lawyers and/or expert witnesses should be able to assess the accuracy and reliability of the evidence in court if the same is challenged by any party to the proceedings.

Oddly, s. 9 of the DNA Bill does not make it mandatory for the Head of DNA Databank to rectify the particulars even if clerical error has occurred or sufficient evidence is produced to him. The section states that he is *entitled to rectify* the particular, but he is not obligated to rectify. As long as the Head of DNA Databank does not exercise or chooses not to exercise his powers under s. 9 for any reason whatsoever, the evidence is conclusive, even if it is blatantly wrong. Is this what is intended by the draftsmen?

A more serious, critical and controversial issue on s. 24 is the use of the phrase "conclusive proof" in that section. This seems to grant the status of an irrebuttable presumption of law to the information from the DNA Databank. It has to be reminded that an irrebuttable presumption is an inference which the law makes so peremptorily that it will not allow the inference to be overturned by any contrary proof, however strong.[26] An irrebuttable presumption of law is almost the same as an indisputable proposition of law. The court shall not allow evidence to be given for the purpose of disapproving the

fact presumed. An arbitrary rule to preclude a party from adducing evidence is an act which can only be justified by the clearest expediency and the soundest policy. In the Evidence Act 1950, there are only three sections that provide the circumstances when this presumption applies - ss. 41, 112 and 113. There is a tendency now to regard such irrebuttable presumptions of law as rebuttable.

Such a peculiar provision of s. 24 does not appear in any of the jurisdictions discussed in this paper. Perhaps, it is non-existence in any DNA laws around the world. One surely would question the reason or intention if such a draconian section is inserted. Several questions arise. Can we trust the enforcement authority with this type of information - which is the genetic code of our being? Can we be sure that the information from the DNA Databank is perfect and correct? Even if this can be assured, does the information from the DNA Databank deserve such special status? Why not make it mandatory for the Head of the DNA Databank to correct data and information which has been proven to be incorrect or inaccurate? It is recommended that s. 24 is to be deleted from the DNA Bill.

Principle 6 - Duration Of Retention Of Personal Data

The sixth principle states that personal data held for any purpose shall not be kept for longer than is necessary for that purpose.

Information On The Indices

The DNA Bill provides for removal of DNA profiles and information from the suspected persons index under s. 18, which states that:

Where an intimate sample or a non-intimate sample has been taken in accordance with this Act from a person reasonably suspected of having committed an offence and -

(a) investigations reveal that he was not involved in the commission of any offence;

(b) the charge against him in respect of any offence is withdrawn;

(c) he is discharged by a court of an offence with which he has been charged, at trial or on appeal;

(d) he is acquitted of an offence with which he has been charged, at trial or on appeal; or

(e) he is not charged in any court for any offence within a period of one year from the date of taking of such sample from him,

the Head of DNA Databank shall, within six months of so being notified by the Officer in Charge of a Police District of the fact referred to in paragraph (a), (b), (c), (d), or (e), remove the DNA profile and any information in relation thereto of such person from the DNA Databank.

It is recommended that the six-months period be shortened to a 1-2 month period. Once there is proof that the suspect is not involved in an offence, such information should ideally be removed immediately. Taking into account the administrative aspect of removal of such information, the recommended period of 1-2 months should be sufficient. The section should also state that the removal must be done in an irreversible and efficient manner so that there is no possibility that such information is able to be retrieved from any archive within or outside DNA Databank. Otherwise, the removal of information would be meaningless.

Section 18 of the DNA Bill only relates to the suspected persons index. There is no provision in the DNA Bill for other indices under s. 3(3) of the DNA Bill. It is opined that similar provision should also apply to other indices but the retention aspect may be different to each index.

In Canada, access to information in the convicted offenders index shall be permanently removed (a) without delay after every order or authorization for the collection of bodily substances from the person to whom the information relates is finally set aside; (b) without delay after the person is finally acquitted of every designated offence in connection with which an order was made or an authorisation was granted; or (c) one year after the day on which the person is discharged absolutely, or three years after the day on which they are discharged conditionally, of a designated offence under s. 730 of the Criminal Code if they are not subject to an order or authorisation that relates to another designated offence and are neither convicted of, nor found not criminally responsible on account of mental disorder for, a designated offence during that period.[27]

Storage And Disposal Of Samples

As for storage and disposal of samples, s. 17 of the DNA Bill states that "(1) The Head of DNA Databank shall safely and securely store all intimate samples and non-intimate samples that are collected for the purpose of forensic DNA analysis, the portions of the samples that the Head of DNA Databank *consider appropriate* and without delay destroy any remaining portions. (2) The procedures for the storage and disposal of an intimate sample and a non-intimate sample shall be as prescribed.

Our view is that s. 17 is subjective in the sense that the destroying of remaining portions of samples is subject to what the Head of DNA Databank *considers appropriate*. Further, the procedures for the storage and disposal of samples "shall be as prescribed". Unfortunately, the DNA Bill does not prescribe the same. Perhaps, it would be prescribed pursuant to s. 26 of the DNA Bill as a regulation. If this is the intention, it is recommended that such regulation be made as soon as the DNA Bill is passed.

In Canada, there is an express provision for destroying the remaining portions. Section 10(1) of the Canadian DNA Identification Act 1998 states that "When bodily substances are transmitted to the Commissioner under s. 487.071 of the Criminal Code or s. 196.22 of the National Defence Act, the Commissioner shall, subject to this section and s. 10.1, safely and securely store, for the purpose of forensic DNA analysis, the portions of the

samples of the bodily substances that the Commissioner considers appropriate and *without delay destroy any remaining portions*." Section 10(6) of the Canadian DNA Identification Act 1998 provides that "The Commissioner may at any time destroy any or all of the stored bodily substances if the Commissioner considers that they are no longer required for the purpose of forensic DNA analysis."

Further to the above, s. 10(7) of the Canadian DNA Identification Act 1998 provides that "The Commissioner shall destroy the stored bodily substances of a person (a) without delay after every order or authorization for the collection of bodily substances from the person is finally set aside; (b) without delay after the person is finally acquitted of every designated offence in connection with which an order was made or an authorization was granted; or (c) one year after the day on which the person is discharged absolutely, or three years after the day on which they are discharged conditionally, of a designated offence under s. 730 of the Criminal Code if they are not subject to an order or authorization that relates to another designated offence and are neither convicted of, nor found not criminally responsible on account of mental disorder for, a designated offence during that period."

In Trinidad & Tobago, s. 32 of the Deoxyribonucleic Acid (DNA) Act 2007 takes the position that where a sample is not destroyed during forensic DNA analysis, the forensic DNA laboratory shall keep the sample for a period of *ten years* from the date on which the analysis was completed and thereafter it shall be destroyed. A court may order that a non-intimate or an intimate sample that has been taken shall not be destroyed if the court is satisfied that the sample might reasonably be required in an investigation or prosecution of that person for an offence or any other person for the same offence or any other offence in respect of the same incident.

In Australia, ss. 464ZFB and 464ZFC of the Crimes Act 1958 provide that the police must without delay destroy, or cause to be destroyed, any sample taken and any related material and information when the court finds a person guilty of an offence, unless an application is made to the court for extension within six months after the final determination of an appeal against conviction or sentence or the expiry of any appeal period in respect of the offence.

Sensibly, a time limit must be set to destroy the DNA sample and/or information, subject to the extension to be given by the court with sufficient reasons that the same is still required in an investigation or prosecution.

Principle 7 - Access To And Correction Of Personal Data

The seventh principle states that the data subject shall be granted access to the information and correct the information where appropriate. Sections 12(5) and 13(5) of the DNA Bill state that a person from whom an intimate or non-intimate sample is taken shall be *entitled to the information* derived from the analysis of the sample taken from him. On the other hand, where the sample is given voluntarily, s. 15(2) (b) of the DNA Bill states that he may make a request to a police officer for *access to the information.*

But the real concern is when there is an error or inaccuracy in the information. Reference is made to s. 9 of the DNA Bill. The data subject may provide sufficient evidence to the Head of DNA Databank to satisfy him that the entry is made incorrectly or there is a clerical error in the information. However, as discussed above, the Head of DNA Databank is *entitled to rectify*, but he is *not obligated* to rectify the particulars in the DNA Databank. The PDP Bill and data protection laws of other jurisdictions recognise that it is the right of a data subject to make corrections to incorrect personal data. The PDP laws make it obligatory on the data user to actually make the necessary corrections, if the data is inaccurate or incorrect. Here lies the contradiction between DNA and PDP. Under the latter, the entitlement/right is given to the data subject, whereas under the former, it is vested with the data user - the Head of DNA Data Bank. This contradiction will have to be resolved.

Principle 8 - Security Of Personal Data

The eighth principle states that all practicable steps to ensure security shall be taken against unauthorised access or accidental access, processing or erasure to alteration, disclosure or destruction of, personal data and against accidental loss of personal data.

Section 17(1) of the DNA Bill expressly provides that the Head of DNA Databank shall *safely and securely* store all intimate samples and non-intimate samples that are collected for the purpose of forensic DNA analysis, the portions of the samples that the Head of DNA Databank considers appropriate. In addition, the functions of the Head of DNA Databank includes "to ensure that DNA profiles and any information in relation thereto are *securely stored and remain confidential*"[28] and "to store and dispose of the intimate sample and non-intimate sample taken for the purposes of forensic DNA analysis in accordance with the provisions of this Act and as prescribed."[29]

The key words in the PDP's eighth principle are, "all practicable steps", which mean that the data user must take measures which commensurate with the risks and the costs to implement the security measures. This would depend on several factors; nature of data, financial capability of the data user, the implication if the data is lost, etc.

In Canada, it is provided that the Commissioner shall, *safely and securely store*, for the purpose of forensic DNA analysis, the portions of the samples of the bodily substances that the Commissioner considers appropriate and without delay destroy any remaining portions.[30] In Trinidad & Tobago, the Custodian shall ensure that DNA data is *securely stored and remains confidential.*[31]

Although s. 17(2) of the DNA Bill states that "the procedures for the storage and disposal of an intimate sample and a non-intimate sample shall be as prescribed", there is currently no prescribed procedure for storage and disposal. Hence, it is recommended that such regulation be made sooner rather than later.

Principle 9 - Information Generally Available

The ninth principle states that all practicable steps shall be taken to ensure that a person can ascertain a data user's policies and practices in relation to personal data and be informed of the kind of personal data held by a data user.

Once the DNA Bill is passed and comes into force, it is pertinent for the DNA Databank to issue their privacy policy and security policy. The scope of works and functions of the DNA Databank should be published and made publicly accessible. To promote better and more transparent operations, there should be public accountability of the officers of DNA Databank.

In Canada, the Commissioner shall, within three months after the end of each fiscal year, submit to the Minister of Public Safety and Emergency Preparedness a report on the operations of the national DNA databank for the year. The Minister shall cause the report of the Commissioner to be tabled in each House of Parliament on any of the first 15 days on which that House is sitting after he or she receives it.[32] Further to that, a review of the provisions and operation of this Act shall be undertaken by any committee of the Senate, of the House of Commons or of both Houses of Parliament that is designated or established for that purpose within five years after this Act comes into force.[33]

In Trinidad & Tobago, the DNA Board shall convene at least four times in every year after the appointment of its members. The DNA Board shall within one month after the end of each meeting, submit to the Minister, a report on its operations. The Minister shall cause the reports of the DNA Board to be laid in Parliament *twice annually*. All members shall hold office for a period of three years and shall be eligible for re-appointment. The President shall terminate the appointment of a member of the DNA Board for inability to discharge the functions of his appointment, whether arising from infirmity of mind or body or any other cause, or for misbehaviour.[34]

It is recommended that the Head of the DNA Databank shall report to the Minister periodically, who shall cause the report to be tabled and discussed in the Parliament. Such provision should be inserted expressly under s. 8 of the DNA Bill.

The Exemption Under s. 73 Of The PDP Bill

At this juncture, it is important for us to review the application of the partial exemption under s. 73 of the PDP Bill, which states, *inter alia,* that personal data held for the *prevention or detection of crime or the apprehension, prosecution, or detection of offenders* is exempt from data protection Principles 3, 4, 7 and the relevant provisions of the Act in any case in which the application of those provisions to the personal data would be *likely to prejudice* any of the said matters. It should be noted that the partial exemption would only apply when the crime fighting initiatives (prevention or detection of crime or the apprehension, prosecution, or detection of offenders) are *"likely to be prejudiced"* by the application of personal data principles. It is opined that partial exemption under s. 73 of the PDP Bill would apply in the situations where crime-fighting initiatives would likely to be prejudiced. However, in situations where crime-fighting initiatives would not likely to be prejudiced, for example the access to and correction of

the voluntary index, such partial exemption should not apply. Therefore, the application of s. 73 of the PDP Bill should strictly subject to the proviso of *"likely to be prejudiced"*.

This partial exemption means that for the purposes of investigation and detection of crime, Principles 3, 4 and 7 of the PDP do not apply to the processing of data for those purposes. Simply put, the data user/Head of DNA Databank does not have to adhere to these principles. The implications are; firstly, data collected for the crime prevention and detection purposes can be used for other related purposes without the consent of the data subject, secondly, the data can be disclosed to other parties without the consent of the data subject, and thirdly, the data subject will have no access to the personal data/information. There is a contradiction between this latter position and the provision of s. 11(c) of the DNA Bill. This section provides that the access to a communication or use of a DNA profile or information is only for the purpose of making the information available to the person to whom the information relates. In short, it allows access, whereas the PDP Bill, in s. 73 mentioned above, denies the data subject from getting access to the data. There are at least two ways to resolve this contradiction. Firstly, by confining s. 11(c) to the voluntary index as provided for in s. 3(3)(g) of the DNA Bill. This means that only in this circumstance is access given to the data subject of his or her DNA profile and information relating to it. Secondly, s. 11 is to be made subject to other law/s.

Concluding Remarks

The use of DNA in combating crime has received judicial recognition. Lord Steyn stated, "It is of paramount importance that law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. It enables the guilty to be detected and the innocent to be rapidly eliminated from enquiries ... But the dramatic breakthrough was the use of DNA techniques since the 1980s. The benefits to the criminal justice system are enormous. For example, recent Home Office statistics show that while the annual detection rate of domestic burglary is only 14%, when DNA is successfully recovered from a crime scene this raises to 48%".[35]

Beginning this year, the law enforcement agencies in Europe are allowed to share DNA information among them. Globally, it is even suggested that the development and potential of an international DNA database is not hard to imagine. DNA law is not new. All states in the U.S. have enacted DNA law, apart from the federal legislation. Many countries in Europe have done the same. So too countries like Australia, New Zealand, Canada, China, Japan and etc.

What is new are the odd provisions in the Malaysia's DNA Bill. Furthermore, the DNA Bill has been tabled without data protection law currently enforced in the country. No attempts, perhaps, have been made to ensure the DNA's compliance with PDP Bill. Consequently, there are grave concerns regarding the provisions of the DNA Bill in relation to data protection principles. Sensibly, PDP Bill should be debated and passed by the Parliament before enacting the DNA Bill in order to protect the privacy rights of

individuals relating to personal data. The proposed DNA law also failed to provide adequate protections/safeguards as provided for in many jurisdictions.

DNA laws aim to strike a balance between the crime investigation needs of the State and the privacy rights of its citizens. How effectively this balance is constructed is a pivotal issue.[36] An example of a sound regime is sometimes explained as one beneath which the innocent have nothing to fear. There is a problematic dichotomy in this reassurance.[37] It is true that an innocent person should be favoured by the use of DNA, as the results should exculpate them from the case at hand. However, the regime also serves to bring more and more such people into the system,[38] thereby minimising their protection against State intrusion into their lives.[39]

Endnotes:

* Faculty of Law, University of Malaya; Adviser to the Ministry of Water, Energy and Communications on Personal Data Protection Bill (2007 - to date).

** Advocate & Solicitor.

1. *Dewan Rakyat* is the House of Representatives of the Malaysian Parliament. The Members of Parliament are addressed as *Yang Berhormat* (Honourable Member) or the abbreviation *"YB"*.

2. See the Hansards for 18, 26, 27 and 28 August 2008 available at the Parliament's website, .

3. Although there is possibility that the proposed Personal Data Protection Bill circulated in 2000 could be amended before it is put to debate in Parliament, the data protection principles should remain substantially the same.

4. Definition of DNA stated in wikipedia's website

5. See the Postnote: The National DNA Database issued by the United Kingdom Parliamentary Office and Science and Technology, February 2006 Number 258, available at the United Kingdom Parliament Website .

6. Act 344 (Revised 1988).

7. Hughes, Gordon, *"Data Protection in Australia"*, (Sydney: The Law Book Company Limited, 1991).

8. "Computer and Privacy" (1975), Cmnd 63'53, para. 26.

9. EU Directive 95/46/EC.

10. Act 388 (Consolidated and revised 1989).

11. Section 12 of the DNA Bill.

12. Section 13 of the DNA Bill.

13. Section 2 of the DNA Bill.

14. Section 12(2)(B) of the DNA Bill.

15. Section 2 of the DNA Bill.

16. Section 2 of the Canadian DNA Identification Act 1998.

17. Section 464 of the Crimes Act 1958.

18. Section 12(6) of the DNA Bill.

19. Section 13(6) of the DNA Bill.

20. Section 464Z(6)(a) of the Crimes Act 1958.

21. In the UK, if a refusal of consent to provide a DNA sample is "without good cause", then the courts may draw "such inferences from the refusal as proper, and the refusal may, on the basis of such inferences, be treated as, or as capable of amounting to, corroboration of any evidence against the suspect.

22. Section 13(7) of the DNA Bill.

23. Section 14 of the DNA Bill.

24. Section 20(2) of the DNA Bill.

25. Section 21(2) of the DNA Bill.

26. See *Sarkar on Evidence* (1990) at p. 40.

27. Section 9(2) of the DNA Identification Act 1998.

28. Section 8(1)(c) of the DNA Bill.

29. Section 8(1)(d) of the DNA Bill.

30. Section 10(1) of the Canadian DNA Identification Act 1998.

31. Section 43(c) of the Trinidad & Tobago Deoxyribonucleic Acid (DNA) Act 2007.

32. Section 13.1 of the Canadian DNA Identification Act 1998.

33. Section 13 of the Canadian DNA Identification Act 1998.

34. Sections 36-38 of the Trinidad & Tobago DNA Identification Act 2007.

35. In the case of *Regina v. Chief Constable of South Yorkshire Police (respondent) ex parte LS* (by his mother and litigation friend JB) (FC) (appellant), *Regina v. Chief Constable of South Yorkshire Police (respondent) ex parte Marper (FC) (Appellant) (Consolidated Appeals)* [2004] UKHL 39 available at http://www.privacyinternational.org/article.shtml? cmd%5B347%5D=x-347-528475

36. Simon J Walsh, *"Legal Perceptions of Forensic DNA Profiling Part 1: A Review of the Legal Literature"*, Forensic Science International, Vol.155, Issue 1, 1 December 2005, at p. 8.

37. *Ibid.*

38. Section 3 of the DNA Bill provides for seven indices and based on international trends it is possible for the indices to be expanded and extended to other groups in the society.

39. *Ibid.*