

INDIA DNA BILL: Uses and restrictions

Uses and restrictions: issues for discussion

- € Should uses for civil cases be allowed (including identification of a person not suspected of being involved in an offence, or identification of non-paternity or relatives)?
- € Is access to databases and samples appropriately restricted?
- € Is there an independent and transparent system of governance, with regular information published e.g. annual reports, minutes of oversight meetings?
- € Is personal identification information stored with DNA profiles adequate or excessive? Is this information sent with samples to laboratories (where it may not be secure) or is there a barcoding system?
- € Is any transfer of data e.g. from police station to lab or database, secure?
- € Are research uses restricted to anonymised verification of database performance (e.g. checking false matches etc.) or is genetic research (e.g. on ethnic appearance, behaviour or health) allowed without consent? Is there any oversight of this?
- € Is familial searching allowed (looking for partial matches with possible relatives of a suspect) and if so, is it restricted e.g. ordered by a court or regulated for use in special cases?
- € Are relevant safeguards proscribed by law and are there appropriate penalties for abuse?
- € Have impacts on children and other vulnerable persons (e.g. mentally ill) been considered?
- € Is there potential for racial bias as to who is on the database? Have ways to minimise bias and discrimination been considered?

Relevant provisions in draft India DNA Bill

Uses of DNA profiles, including identification of a person

In Chapter VII, Section 35, the Bill states that when a DNA profile is received for entry in the DNA Data Bank it shall be compared with the DNA profiles in the DNA Data Bank in order to determine whether it is already in the DNA Data Bank. In relation to the investigation or prosecution of a criminal offence, information can then be passed to a court, tribunal, law enforcement agency or DNA laboratory. In relation to other cases, information can be passed to an authorised official. A similar provision in Section 36 allows the same process to occur on receipt of a DNA profile from a foreign government. However, these Sections do not limit the comparisons that can be made between DNA profiles from different sources.

Legitimate comparisons for the purpose of solving crimes could include: (1) a search of a new crime scene DNA profile against the crime scene index to establish possible links between multiple crimes; (2) a search of a new crime scene profile against the offenders index to look for matches which may indicate that a previously convicted offender is linked to a new crime; (3) a search of a new offender's DNA profile against all stored crime scene DNA profiles to look for matches which may indicate that the offender is linked to crimes other than that for which they have been convicted. These searches could be extended to include suspects as well as offenders, but this then raises questions about the circumstances in which an unconvicted person's profile should be compared with stored crime scene DNA profiles from other crimes and/or retained so that new crime scene profiles from future crimes can also be compared to it. In most countries there are restrictions on the extent to which unconvicted persons' DNA profiles can be searched and/or stored.

The wording in the Bill also suggests that crime scene DNA profiles would be searched against the missing persons' index and volunteers' index, as well as any other index that may be set up under 32(3)(g). This is not normal practice in other countries since these persons are not suspects for a

crime. For example, in the UK, DNA profiles on the Police Elimination Database are stored separately from those of convicted persons and suspects and crime scene profiles are not routinely against the database, but only compared when needed to eliminate a specific officer when they have attended (and may have contaminated) a crime scene.

Other legitimate uses might include searching the DNA profile of an unknown deceased person against all indices, or searching the profile of an abandoned or disputed child against the missing person's index. In the latter case, special attention would need to be given to the best interests of the child, the UN Convention on the Rights of the Child, and the consent of interested parties (including the child and persons claiming to be parents, or not parents, of the child). It is normal practice in most countries to keep missing persons' DNA databases separate from criminal DNA databases in view of these sensitive issues.

Finally, the wording in the Bill seems to imply that a search of a new individual's DNA profile should be made against all the stored indices, with a view to establishing whether that individual is already on the database. Because it is proposed that there are multiple indices in the DNA Data Bank, this could lead to breaches of privacy such as police identifying a suspect as having previously being involved in a paternity dispute. It is unclear whether the volunteers' index will include police officers and laboratory workers, whose DNA profiles must be retained for elimination purposes (because they may inadvertently contaminate evidence at the crime scene or in the lab). If so, they may also be vulnerable to breaches of privacy. There are likely to be "adventitious matches" (false matches which occur purely by chance) between newly added individuals' profiles and stored profiles and this must be considered when conclusions are drawn about whether an individual is already on the database. In addition, individuals may use false names and there will be more than one individual with the same name. In the UK, fingerprints are used as a second check to confirm whether the person with a record on the DNA database is the same individual as the suspect: this also allows adventitious matches to be identified.

The Bill currently allows (Schedule Part 1.C) uses for civil cases and matters including "Issues relating to establishment of individual identity" as well as "Parental dispute" and "Issues relating to pedigree". This raises the prospect of routine use of the database to track individuals (for example, by collecting DNA from tea cups left at a political meeting and searching the profiles against the DNA Data Bank to identify who was present) or to identify their relatives (by using "familial searching", which looks for partial matches between a DNA profile and the DNA profiles of others who may be related). Such searches would appear to be able to be conducted in relation to innocent individuals (including volunteers, missing persons and unconvicted suspects) as well as convicted persons. It is unclear whether volunteers include police officers and laboratory employees: if so, they could also be vulnerable to anyone who infiltrates the system seeking to identify and track them or their relatives. At the same time, it is not obvious what would prevent a police officer from submitting a sample in order to seek to identify paternity of their own child, or another person (including officials, neighbours or family members etc.).

These problems are exacerbated by the provision in Section 36 to allow the submission of DNA profiles from other countries: there appears to be no restriction on what profiles can be submitted. For example, a legitimate use would be to search for a match with a crime scene DNA profile from a serious crime committed in another country. However, other uses might involve trying to track political opponents or their relatives. Other countries might also regard some activities as serious crimes when they are not considered crimes in India or are very differently defined (e.g. blasphemy, adultery), and some individuals with legitimate claims for political asylum might be regarded as criminals in their own country. Human rights checks are therefore needed on any proposed uses. As worded, a legitimate use might be searching for a missing child (Schedule Part 1.D(iii)): however such searches could be conducted on behalf of an abuser seeking to trace a child who has legitimately

fled to another country.

Research uses are mentioned in Section 40(e): *"for creation and maintenance of a population statistics database that is to be used, as prescribed, for the purposes of identification research, protocol development or quality control, provided that it does not contain and personally identifiable information and does not violate ethical norms"*. This is somewhat vague about what "ethical norms" are (and who will decide): there is a danger it leaves the door open to stored DNA samples or profiles being used to try to predict ethnicity or appearance under the category "identification research".

It is unclear what rules on searches (if any) apply to the State DNA Banks set up under 32(1) and (2), since Sections (35) and (36) appear to refer to the National DNA Databank (which is under the control of the DNA Data Bank Manager).

Roles of the Board and Government

Chapter III: DNA Profiling Board creates a Board to oversee the operation of the DNA database. It outlines membership and powers. Rules of procedure will be created by regulations. Direct and indirect interests in any matters being considered are supposed to be recorded (III.7). The Government may remove members with financial interests that prejudice their functions or who abuse their position (III.8). Chapter IX requires the Board to publish an annual report giving a full account of its activities and for this to be audited and placed before parliament. However, more detail could be provided on what should be included in the annual report. There is no stated requirement for minutes of Board meetings (including declarations of interest) to be published.

Chapter VII Article 33 requires a DNA Data Bank Manager to be appointed to manage operations of the National DNA Data Bank. The Board will determine the number, nature and categories of other officers and employees with approval of the Government (VII.34). However, it is not clear who is responsible for the State DNA Banks set up under Article 32.

The Government, Board, or officers and members, cannot be prosecuted provided they have acted in good faith (XI.60).

Central Government can, by notification, supersede the Board for up to six months (XI.62).

Central Government can, by notification, make rules governing a wide range of issues listed in XI.65 (2), including conditions for approvals of laboratories, the manner for expungements of records and manner in which access to data shall be restricted etc. This includes (in XI.65(2)(g)) rules allowing "other purposes" for which information on DNA profiles, samples and DNA identification records can be made available under subsection (g) of section 40 and "any other matter" (XI.65(2)(l)). This would appear to allow uses of the database to be extended by Government without adequate oversight.

The Board can, by notification, make regulations and rules on a wide range of matters listed under XI.66(2). As well as matters regarding their own meetings and standards for laboratories this includes extending the list of applicable instances of human DNA profiling and the sources of collection of DNA samples contained in the Schedule (XI.66(2)(d)); adding other DNA indices in addition to those listed in the Bill (XI.66(2)(y)); adding other civil purposes and matters in addition to identification of victims of accidents, disasters or missing persons and the civil disputes and matters listed in the Schedule Part I.C (XI.66(2)); authorising other persons to take non-intimate samples (XI.66(2)(zh)). This would appear to allow uses of the database to be extended by the Board without adequate oversight.

Rules and regulations made under the Act must be laid before parliament for a total period of thirty days but can only be rejected if both houses agree the rule or regulation shall not be made (XI.6)

Penalties

Chapter X outlines Offences and Penalties. Wilful disclosure of identifiable DNA information contained in the DNA Data Bank to any person not entitled to receive it; wilfully obtaining this information without authorisation, accessing information not in accordance with the Act; knowingly providing a DNA sample or result to a person not authorised to use it; and knowingly and intentionally destroying, altering or tampering with biological evidence; are all offences which may receive a prison term of one to three months plus a fine. Directors and managers can be guilty of offences if negligent. Complaints to court must be made by the Government or its officer or by the Board, but individuals can approach a court if the Government or Board take no action within three months.

These sanctions are important but their impact may be limited by the existing very broad potential uses of the database and possible wide range of authorised persons, together with the powers of the Government and Board to extend both access and uses. To be meaningful, the Bill needs to be clearer and more tightly restricted regarding what the authorised uses and persons are.

Examples of misuse and bad practice

Police DNA database 'is spiralling out of control'. The Observer. 16th July 2006.

<http://www.guardian.co.uk/uk/2006/jul/16/ukcrime.immigrationpolicy>

Public concerns about lack of independence of the DNA database. UK Human Genetics Commission Citizens' Inquiry 2008: <http://www.hgc.gov.uk/Client/document.asp?DocId=158&CAtegorId=8>

Police in the UK are now selling records of arrest to individuals who are required to provide them to employers and for some visa applications. These records used to be deleted but are now retained so they can be linked to DNA profiles on the DNA database.

Body in charge of UK policing policy is now an £18m-a-year brand charging the public £70 for a 60p criminal records check. Daily Mail, 15th February 2009. <http://www.dailymail.co.uk/news/article-1145581/Body-charge-UK-policing-policy-18m-year-brand-charging-public-70-60p-criminal-records-check.html>

Fears over innocent Britons' DNA being given to European police forces. Daily Mail. 9th May 2007.

<http://www.dailymail.co.uk/news/article-453739/Fears-innocent-Britons-DNA-given-European-police-forces.html>

DNA of 37% of black men held by police. The Guardian. 5th January 2006.

<http://www.guardian.co.uk/world/2006/jan/05/race.ukcrime>

Three in four young black men on the DNA Database. The Telegraph. 5th November 2006.

<http://www.telegraph.co.uk/news/uknews/1533295/Three-in-four-young-black-men-on-the-DNA-database.html>

DNA database scandal is damaging UK race relations says expert. The Voice, 17th August 2009.

<http://www.voice-online.co.uk/content.php?show=16083>

Examples of good practice

Following concerns about the misuse of the UK DNA Database for genetic research without consent, the government set up a DNA Database Ethics Board. This is separate from the Board manages the DNA database: <http://www.homeoffice.gov.uk/agencies-public-bodies/fsr/ndnad-ethics-group/>