**Comments on India's Human DNA Profiling Bill (June 2015 version)**

**GeneWatch UK**
**August 2015**

GeneWatch UK is a participant in the Forensic Genetics Policy Initiative (FGPI), a joint initiative of GeneWatch UK, the Council of Responsible Genetics and Privacy International. FGPI maintains a website[1] and a wiki of national and international policies, debates and laws regarding forensic DNA databases[2], and has published a preliminary international review of ethical and privacy standards. We are currently working on a more substantive analysis of best practice for DNA databases worldwide. GeneWatch UK has provided expert evidence on DNA databases to the European Court of Human Rights and to the British Parliament. GeneWatch UK and the Council for Responsible Genetics visited India in September 2012 to discuss the issues raised by an earlier draft of the Human DNA Profiling Bill. This consultation response draws on an earlier analysis by the Council of Repsonsible Genetics[3], which raised many issues which have yet to be addressed.

We welcome the opportunity to input to this consultation. However, due to the short timeframe and the many issues raised by the draft Bill we cannot guarantee that our response is fully comprehensive. We are happy to provide further information on request.

## 1. Overview of concerns about the Bill

The FGPI's main concerns about the Bill are outlined below. Although there have been some welcome changes since earlier drafts, many concerns remain.

### 1.1 Collection

There are limited restrictions on when DNA samples can be collected from individuals in the Bill, as a sample can be collected from a suspect for any cognizable offence without any judicial or other oversight. Although this is an improvement on earlier versions of the Bill, which referred to suspects for any offence (however minor), the number of persons potentially involved remains very large, as arrest for a cognizable offence with no DNA evidence involved could still lead to an individual's sample being taken. Lack of any judicial or other oversight would also allow people to be arrested simply in order to obtain their DNA. Samples can also be taken from volunteers, which could potentially be anyone in India: there is no specific requirement in the text of the Bill for the individual or their parent or guardian to give informed consent. No process for sample collection is specified – this is left to the Board. Although intimate samples will require a medical professional there is no specific requirement for informed consent.

### 1.2 Retention

The Bill relates to biological samples (such as cells collected from suspects on mouth swabs) and DNA profiles (numbers that result from DNA analysis, which can be stored on a computer).

#### *1.2.1 Retention of DNA profiles*

There is no restriction of the analysis i.e. it is not limited to forensic DNA profiles (a limited string of numbers used for identification purposes) based on non-coding DNA: this means unnecessary private information could be revealed relating to health or other characteristics.

The Bill creates indices for information based on DNA analysis from: crime scenes, suspects, offenders, missing persons, unknown deceased persons, volunteers and "such other indices as may be specified by regulations". The need for staff elimination databases is not recognised, but this is important as relevant members of police, medical examiners and laboratory workers may inadvertently contaminate samples with their own DNA. It is best practice to create a separate database for missing persons and their relatives, rather than to include them on a criminal DNA

database, and to use volunteers' DNA profiles for elimination purposes only in relation to the specific offence for which they have been collected.
Offenders are incorrectly defined to include persons against whom a criminal proceeding is pending in a court of law. This means that some persons who are suspects awaiting trial are wrongly categorised as offenders in the Bill, although they may be innocent.
The Bill allows for DNA profiles from these suspects (i.e. those wrongly classified as offenders) to be removed from the database if they are found not guilty, or for other offenders to have DNA profiles removed if their conviction is squashed. However, removal requires the Board to receive a court order: the onus should be on the Board or DNA Databank manager to remove profiles otherwise innocent people's DNA profiles are likely to be retained, perhaps indefinitely, if there are bureaucratic delays.
There are no provisions for the removal of DNA profiles taken from suspects who are not proceeded against, volunteers, missing persons and their relatives, or any other individual that may be added if the scope is expanded by means of regulations: this means that information from innocent people could be retained against their wishes.
Persons, including children, who are convicted of minor cognizable offences will have their information retained indefinitely.
The Bill creates powers for regional and state databases to be set up but does not specify whether DNA profiles stored by regions or states will be retained indefinitely or can be deleted.

***1.2.2 Retention of DNA samples***

There is no provision for the destruction of biological samples collected from individuals (which might be held centrally, or at regional or state level). Samples contain significant personal information which is unnecessary for identification purposes and their destruction is an important privacy protection. The Bill gives the DNA Profiling Board the powers to develop guidelines for storage and destruction of biological samples, rather than restricting storage in law.

**1.3 Uses**

Privacy protection requires data to be used only for the purpose for which it was originally collected. However, the Bill allows a very broad list of uses, including in civil proceedings – which is likely to include identifying family relationships such as non-paternity. The Bill also allows the Government and the DNA Profiling Board to add to this list of uses without full parliamentary scrutiny. The definition of a "DNA profile" does not restrict the analysis to forensic DNA profiles: this means additional information, such as health-related information, could be analysed and stored against the wishes of the individual, even though such information plays no role in solving crimes. In addition, there is no restriction on the circumstances in which foreign governments may request stored DNA profiles, including from innocent persons. It is not only the privacy of convicted people that is at risk. Innocent people, including volunteers, relatives of missing persons, or people falsely accused of a crime could have their privacy breached in this way if no legal restriction on uses is in place. These provisions may also pose a risk to Indian security if DNA profiles of security personnel or politicians (or their family members) are inadvertently shared with foreign services.

**1.4 Oversight**

The DNA Profiling Board is given very broad powers. It is also made exempt from civil or criminal proceedings. Allowing new indices to be added to the database, or new uses of the data to be developed, undermines the basis on which volunteers may give consent and may render any human rights protections meaningless. The indices and uses should be a matter for parliament to decide in the legislation and should not be left to the Government or the Board to amend later on.
In the Bill, the Board acts as the manager and advocate of the database as well as its regulator. It would be better to separate these roles and create a separate Forensic Science Regulator which can make an independent investigation if anything goes wrong, and an Ethics and Privacy Regulator, to

provide independent scrutiny of ethical and privacy issues, including compliance with human rights safeguards.
Although offences and penalties are defined, the Government or Board takes the lead in bringing cases. Best practice would involve an independent regulator who can be approached by members of the public, so there is a quick remedy for citizens who believe their DNA has been collected, used or retained unlawfully. This section also allows the Board to profit from its activities without paying any tax.
It is unclear what, if any, safeguards or oversight apply to regional or state databases or laboratories, as penalties refer to "the DNA databank" only.

**1.5 Lack of provisions to prevent miscarriages of justice**
Although the preamble to the Bill states that it lays down standards for the "custody trail from collection to reporting", in fact it only regulates laboratories, rather than all aspects of the collection of DNA from individuals or crime scenes and use of DNA evidence in court. This leads to some important gaps in provisions which are necessary to prevent errors and mistakes and avoid miscarriages of justice. It is important to note that many countries also require prosecutions to submit corroborating evidence and not be based on a DNA match alone. For example, in the UK this requirement is contained in Crown Prosecution Service Guidelines.[4] This is an important additional safeguard to prevent miscarriages of justice.

## 2. Specific comments on the Bill (June 2015 version)

The following changes are proposed to be consistent with best practice. Additional safeguards regarding the use of DNA evidence in court and the need for corroborating evidence in court are not dealt with in these more detailed comments, as it may be more appropriate to introduce them via amendments to other legislation.

### 2.1 Chapter I: Preliminary

Clause 1(3) allows different commencement dates for different clauses. It may be appropriate to bring some provisions into force before others, but only if safeguards (such as quality assurance for laboratories) are implemented before collection of DNA profiles for the database begins.

Clause 2(1)(i) and (j): "DNA Profile" should specify that the analysis is based on non-coding regions of the DNA, as a safeguard to prevent the analysis and storage of private health-related information without consent. Example wording: *"DNA profile", in relation to a person, means information comprising a set of identification characteristics* ***of the non-coding part of DNA*** *derived from an examination and analysis of a sample of biological material that is clearly identifiable as relating to the person and that is capable of comparison with similar information derived from an examination and analysis of another sample of biological material for the purpose of determining whether or not that other sample could relate to that person*. Criminal Justice (Forensic Evidence and DNA Database System) Act 2014, Ireland [page 13, emphasis added].[5]

Clause 2(1) (o): Serious consideration should be given to creating a separate missing persons database, rather than including missing persons and their relatives in a criminal DNA database. A decision to keep these databases separate has already been made in the UK: "*In certain circumstances, volunteer samples may also be requested from individuals, together with consent for the resulting profile to be searched and retained on a DNA database. Such samples are only requested in a relatively small number of cases, for example, in missing persons enquiries and from potential vulnerable persons. Where consent to retention is also provided, these volunteer profiles will be loaded to the Missing Persons DNA Database (MPDD) or the Vulnerable Persons Database*

*(VPDD). Volunteer samples are also sometimes taken from previously unsampled registered sex offenders and the resulting profiles are loaded to the NDNAD* [National DNA Database]" (para 2.10 NDNAD biennial report 2009-11).[6] The advantage of keeping these databases separate from other DNA databases is to reassure relatives of missing persons that the use of their stored profiles will be restricted to searching for their missing relative (see further comments on searches below). The definition of the missing persons' index or database should in any case include a reference to the requirement for fully informed consent from relatives. For example, change to: *"missing persons database" means a database of DNA profiles derived from forensic material taken from-*
*(i) the persons who are missing; and*
*(ii) volunteers who are relatives of missing persons and who have given fully informed consent for the entry and retention of their DNA profiles in the database. Consent of volunteers may be withdrawn at any time, resulting in removal of their DNA profile from the database.*
A requirement for fully informed consent is an internationally recognised standard, and the process for obtaining consent should be outlined in the main text of the Bill.
A definition of a "missing person" should also be added. For example Ireland's Act uses:
*"missing person" means a person who, whether before or after the commencement of this section, is observed to be missing from his or her normal patterns of life, in relation to whom those persons who are likely to have heard from the person are unaware of the whereabouts of the person and that the circumstances of the person being missing raises concerns for his or her safety and well-being*.
Without a definition, the state could use the missing person's database or index to track persons of interest (such as political opponents) in circumstances where a person has moved to an unknown location but there are no concerns for their safety or well-being. Concern about this potential abuse is exacerbated by failure to include explicit requirements for fully informed consent in the Bill.

Clause 2(1)(x). As argued further below, the Board should implement, not make the regulations, as in principle the roles of overseeing and regulating the database should be separated. Some matters on which the Board is given powers to regulate in this draft of the Bill should remain decisions for parliament, whilst others should be undertaken by relevant regulatory bodies (as one potential approach to separating these roles, we propose a Forensic Science Regulator and an Ethics and Privacy Regulator, below).

Clause 2(1)(q) "Offender" should be defined to include only persons convicted of a specified criminal offence. Persons "*undertrial charged with a specified offence*" are not offenders, they are suspects, since some such persons are innocent and will not be convicted.

Clause 2(1) (z) In the Bill, "specified offence" means an offence which is cognizable offence listed under the heading "Part I – OFFENCES UNDER THE INDIAN PENAL CODE" in the First Schedule of the Code of Criminal Procedure, 1973.[7] Cognizable offence means a police officer has the authority to make an arrest without a warrant. In India, crimes like rape, murder, theft etc. are considered cognizable, and crimes like public nuisance, simple hurt, mischief etc. are considered non-cognizable. Nevertheless, this provision allows collection of DNA from an extremely broad category of persons, the majority of whom will not require their DNA to be collected for any purpose in relation to their trial, since DNA evidence is not relevant to most offences (i.e. a crime scene DNA profile is not generally available). For example, crimes involving unlawful assembly or taking a gratification as a public servant do not normally involve DNA evidence and are examples of types of cognizable offence where the collection of DNA could be abused (for example to track political opponents and identify their relatives). The more expansive the definition of a "specified offence" the larger the DNA database will be, increasing costs, the risk of errors, and the potential for abuse. If the category of "specified offences" is instead restricted to offences for which DNA is most likely to be relevant and for which resources are available to collected DNA from crime scenes it is more likely that the database will be cost-effective and the risk of errors and abuse can be minimised. A complementary

approach to prevent uncontrolled expansion of the database would be to require judicial oversight of when DNA samples are taken from individuals, in order to ensure that they are relevant to the investigation. For example, in Thogorani Alias K. Damayanti v. State of Orissa and Ors, 2004 Cri. LJ 4003 (Ori), the Orissa High Court affirmed the legality of ordering a DNA test in criminal cases to ascertain the involvement of persons accused. Refusal to cooperate would result in an adverse inference drawn against the accused. After weighing the privacy concerns involved, the court laid down the following considerations as relevant before the DNA test could be ordered: "(i) the extent to which the accused may have participated in the commission of the crime; (ii) the gravity of the offence and the circumstances in which it is committed; (iii) age, physical and mental health of the accused to the extent they are known; (iv) whether there are less intrusive and practical ways of collecting evidence tending to confirm or disprove the involvement of the accused in the crime; (v) the reasons, if any, for the accused for refusing consent." The Bill as drafted appears to leave these considerations to the police, or in effect to omit them altogether, rather than requiring the opinion of a court.

Clause 2(1) (zd) The "unknown deceased persons' index" should be restricted to those cases authorised by a coroner, where the coroner has reason to believe that the entry of the profile in the database may assist in identifying that person (see, for example, Section 50 or Ireland's DNA Act). Failure to include any authorisation mechanism leaves the testing of deceased persons open to abuse, for example as a surreptitious means to track down a relative of the deceased or identify non-paternity within a family. Consent from the relatives of the deceased person should be sought and provisions for this included in the main text of the Bill.

Clause 2(1) (za): The definition of "suspect" has rightly been changed from earlier versions of the draft Bill, so that it means a person suspected of having committed a specified offence. This change is essential to be consistent with the definition of an offender and the Bill's intent to collect DNA in relation to specified offences and not to minor (including non-cognizable) offences, otherwise vast numbers of people would have their DNA collected and their DNA profiles entered on the database, even when this information is not relevant to solving crimes. However, the category of specified offences is still too broad (see comments on Clause 2(1)(z)) and there is a need for oversight of police decisions to avoid them arresting persons simply to obtain their DNA.

Clause 2(1)(zf) and (zg): These clauses should make reference to informed consent. Example wording: *"volunteer" means a person who gives their fully informed consent to undergo a DNA profiling procedure or, in case of a child or incapable person, his/her parent or guardian provides fully informed consent to submit the child or the incapable person to undergo a DNA profiling procedure, taking account of the best interests of the child or incapable person*. It should be noted that consent to having a sample taken, analysed and used in relation to investigation of a particular offence is not the same as consent to entry on the database, which (if it happens at all) should require a separate consent procedure. Serious consideration should be given to removing the "volunteers' index" altogether: in the UK a study found that, although collecting volunteers' samples during a specific investigation is necessary and important, storing these DNA profiles brought no added benefit. As a result, volunteers' DNA profiles are no longer stored on the UK National DNA database and are deleted following the completion of the specific investigation in which they were involved. The National DNA Database (NDNAD) Ethics Group stated in their 2008 report (paragraph 5.4): "*Importantly, the work presented to the DNA Strategy Board illustrated that DNA matches between volunteer profiles and crime stains are satisfactorily achievable irrespective of whether or not the volunteer profiles are loaded from the analysing laboratory to the NDNAD. With the exception of sex offenders (who are sometimes sampled under the volunteer procedure), on the results to date, all of the matches useful to the police would have been obtained without speculative searching of the NDNAD. There would therefore be no loss to operational policing if, for the majority of crimes,*

*volunteer samples were not loaded onto the NDNAD and were used only in relation to the investigation of the crime for which they were obtained*".[8] The UK National DNA Database Biennial Report 2009-2011 states: "*It has decided that in future, volunteers who consent to provide a DNA sample for elimination purposes should no longer be asked to provide consent for their profile to be loaded to the NDNAD and these profiles will not be loaded*" (paragraph 2.9)[9]. The definition of a "volunteer" must in any case include a requirement to give fully informed consent to having their DNA sample collected and analysed. In relation to children or others lacking capacity to give consent, it should be clear that their parents/guardians must act in their best interests. If a volunteers' index is maintained, despite the lack of evidence of usefulness, it should at minimum be redefined to include a specific requirement for consent e.g. as *an index of DNA profiles derived from bodily samples taken from volunteers who have given fully informed consent for their DNA profiles to be entered and retained in the DNA databank and subject to speculative searches*. If such DNA profiles are added to a database, it should also be specified that consent can be withdrawn at any time, resulting in removal from the database.

Clause 2(1): Missing definitions: the need for staff elimination databases and a definition of the persons that should be included, e.g. "police, laboratory and medical staff whose DNA profiles are required for elimination purposes, due to their direct involvement in DNA collection or analysis", have been omitted from the Bill. Whilst volunteers are members of the public (often victims of a crime) whose DNA profiles are needed for elimination purposes for a specific offence, there is a different category of persons, i.e. police, laboratory and medical workers, whose DNA profiles should be stored on a database if their work might lead to contamination of crime scene samples, either during the process of examination of a crime scene (where a police officer might leave their DNA) or during the laboratory analysis of samples. Strictly speaking these persons are not volunteers, as providing a sample may be a condition of their work, although their fully informed consent should be sought before their sample is taken. Databases of their DNA profiles are usually kept on separate elimination databases, as these persons are neither suspects nor convicted persons: in the case of medical and laboratory staff these databases may be managed by the hospital or laboratory where they work, rather than being shared with the central of state government. Provisions should be also made for deletion of staff DNA profiles when retention is no longer necessary (see comments on Part V). The UK's Forensic Science Regulator has published a detailed report on the importance of elimination databases.[10] The costs of establishing one or more Laboratory Elimination Database(s) (LEDs), Police Elimination Database(s) (PEDs) and Medical Examiners Elimination Database(s) (MedExDs) should be included in the costs of implementing the Bill. As for missing persons, best practice would maintain these databases separately from the criminal DNA database and restrict searches to those that are necessary to identify contamination.

### 2.2 Chapter II: DNA Profiling Board

Clause 12(4) allows the Board to hold consultations, but does not require it to do so. Consultations should be required wherever a proposed measure will make an impact on the rights or interests of persons. The provisions should include a requirement to consult the Forensic Science Regulator and/or Ethics and Privacy Regulator (as proposed below) when relevant, and for those bodies to consult persons who may be affected by the changes.

Clause 13 gives a very broad range of functions to the Board. In effect the Board is manager of the database, responsible for: (i) its establishment, day-to-day operations, security of data, and role in solving crimes; (ii) the technical and quality aspects of collection analysis and use of DNA from crime scenes and individuals; and (iii) the development of, and compliance with, measures to protect privacy and human rights and ethical standards. Experience in the UK suggests it is better to

separate these roles so that the public trust that the database is subjected to adequate independent scrutiny and any conflicts-of-interest are avoided. This would involve establishing three bodies, rather than one: (i) a DNA Database Board to oversee the database; (ii) a Forensic Science Regulator to set technical standards for laboratories and (more broadly) for the entire custody trail from collection to reporting (as stated in the preamble to the bill) and to check compliance and investigate mistakes (see, for example, the UK Forensic Science Regulator[11]); and (iii) an Ethics and Privacy Regulator to establish and scrutinise safeguards to protect privacy, human rights and ethical standards (in the UK this role is played by two separate bodies, the Information Commissioner, who has legal powers to regulate data protection, and an ethics board, which advises the DNA Database Board on ethical issues: there is also a Biometrics Commissioner who advises on deletion of DNA profiles and destruction of samples). Under the approach proposed here, the DNA Database Board would remain responsible for running the database and implementing standards to prevent miscarriages of justice and protect human rights, but the Forensic Science Regulator and Ethics and Privacy Regulator would set and independently scrutinise the implementation of those standards.
Functions retained by the DNA Database Board would then include Clause 13(b), part of (d) (supervising DNA laboratories and DNA databanks), and part of (f) (conducting DNA training programmes). Functions for the Forensic Science Regulator would include Clause 13(a), (c), part of (d) (monitoring inspection and assessment of DNA laboratories and DNA databanks in relation to technical, scientific and quality assurance issues), (e), part of (f) (monitoring, regulating, certifying and auditing of DNA training programmes in relation to technical and scientific aspects), part of (h) (laying down technical procedures for the communication of information relating to the DNA profile in civil and criminal proceedings and for the investigation of crimes by law enforcement and other agencies), (i), (j), part of (n) (technical aspects), part of (q) (technical aspects), and part of (r) (technical aspects). Clause 58(2)(j) to (s), and (v), are also matters that should be defined by an independent Forensic Science Regulator, rather than the Board.
The Ethics and Privacy Regulator's functions would include part of (f) (monitoring, regulating, certifying and auditing of DNA training programmes in relation to ethical and privacy aspects), part of (h) (laying down ethical and privacy standards for the communication of information relating to the DNA profile in civil and criminal proceedings and for the investigation of crimes by law enforcement and other agencies), (l), part of (n) (ethical and privacy aspects), (p), part of (q) (ethical and privacy aspects), part of (r) (ethical and privacy aspects), (t). Rules for the matters in Clause 57(c) and (d) should be matters for the proposed Ethics and Privacy Regulator, rather than the Government.
Functions undertaken by all three bodies would include (g), (j), (m), (o), (s), (u), (v) (in relation to their particular areas of expertise).
Note that the roles of the proposed bodies in functions (t) (framing guidelines for the storage of biological samples and their destruction) and (s) (advising Central Government on any modifications required to be made in the lists contained in the Schedule) should be restricted, as discussed below.
A requirement to destroy individuals' samples within a limited time should be included as a specific requirement in the Bill to protect privacy (see comment on Clause (22), and lists should not be modified except through a process involving full scrutiny by parliament should Government propose future revisions to the Act once adopted (see comment on Clause 25(1)(g)). Allowing Government to add lists without full parliamentary scrutiny creates an unacceptable risk of "mission creep" which will lead to significant mistrust.

### 2.3 Chapter III: Approval of DNA Laboratories

Clause 14: The role of approving laboratories should be undertaken by the Forensic Science Regulator, as proposed above, not by the DNA Database Board.
Clause 15: Should require all laboratories to be approved before beginning the collection of DNA profiles for the DNA Databanks.

Clause 18: The body responsible for hearing appeals should be specified in the Bill, not left until a later date, and should not be the Government itself. The public must have confidence that laboratories are audited to international standards and that the decision to allow a laboratory to continue operating cannot be influenced by individuals or companies lobbying Government.

### 2.4 Chapter IV: Standards, Quality Control and Quality Assurance Obligations of DNA Laboratory and Infrastructure and Training

Clause 22: This clause should also require laboratories to destroy spare biological samples collected from individuals once the DNA profiles used for identification purposes have been obtained, not later than six months after the samples have been collected. Destruction of samples prevents further analysis to identify other genetic characteristics, e.g. in relation to health, and is therefore an important privacy protection. Note: samples from crime scenes should not be destroyed as new analysis may be required by the court or to investigate possible miscarriages of justice. A wrongly accused or convicted individual, on the other hand, can always provide a new sample for analysis.

Clause 23(1) should specify that samples from crime scenes must be collected by persons trained in crime scene examination and acting in accordance with regulations designed to (i) establish a clear audit trail for evidence from the crime scene to the court and (ii) minimise the risk of contamination. It is widely acknowledged that ISO/IEC17020 – "General criteria for the operation of various types of bodies performing inspection" is the international quality standard most appropriate to scenes of crime work. Including a commitment to meeting international standards for crime scene examination is necessary to fulfil the purpose stated in the preamble to the Bill of covering the "custody trail from collection to reporting". Many errors may occur before samples reach the laboratory if the correct procedures are not in place e.g. mix-ups of samples so it is unclear where they came from, contamination of samples (e.g. so that DNA from an innocent person is transferred to a murder weapon inadvertently when evidence is moved from a crime scene). This kind of error can lead to serious miscarriages of justice, including imprisonment of innocent persons or failure to identify the true perpetrator due to loss or contamination of evidence. The UK Forensic Science Regulator has published a useful report on examination of crime scenes.[12]

Clause 23: Clause 23(2) should specify that the collection of intimate samples requires the fully informed consent of the individual (or of their parent or guardian in the case of children and incapacitated persons acting in the best interests of the child or incapacitated person). As far as we are aware, no other country allows intimate samples (e.g. from genital areas) to be collected without consent. Clause 23 should also specify the circumstances under which non-intimate samples can be taken from individuals, including when and where (e.g. in secure location when the individual is under detention by the police or in a medical facility i.e. not on the street) and the requirements for consent (including how consent will be obtained for children and incapacitated persons) or alternative means of oversight in the circumstances where a sample (such as hair) may be taken without consent (such as a court order). It should also require provision of information for all persons from whom DNA is taken, regarding their rights and future uses of their DNA sample and profile.

Missing provisions: The defendant should have a right to have a second sample to be taken from him/her prior to trial, as a safeguard against mixed-up samples (i.e. a situation where a different person's DNA sample was analysed and has been wrongly associated with the defendant). This kind of mistake may occur for a variety of reasons, not only due to laboratory error: for example the suspect may simply share a name and some identifying characteristics with a person whose stored DNA profile has matched a crime scene DNA profile, and may therefore be wrongly arrested by the

police. Such a measure does not prevent crime scene sample mix-ups or contamination (which are more common), but it can help to avoid one obvious potential source of error.

### 2.5 Chapter V: DNA Data Bank

Clause 24 includes powers for the Central Government to create Regional DNA Databanks, as well as a National DNA Data Bank and for states to create State DNA Databanks. However, it is unclear whether all the regulatory procedures and safeguards in the Bill will apply to all the Databanks. For example, Clause 26 specifies the process for appointing a National DNA Databank manager but is silent on the process for the other data banks. Most importantly, provisions for the deletion of DNA profiles from the National DNA Databank should apply to all Databanks. Otherwise the privacy of innocent persons is not protected, as a DNA profile deleted from the National DNA Databank may still be retained on regional or state databanks.
In addition, the role of the Regional DNA Databanks is not specified e.g. whether they send copies of DNA profiles to the National DNA Databank.

Clause 25 (1): Clause 25(1)(g), which allows the addition of new indices, should be deleted, since an important element of safeguards to protect privacy and human rights is the limitation through legislation of the purposes for which the data can be collected, retained and used. This is also important to maintain public trust and the confidence of persons who may be asked to volunteer their DNA. As noted in the comments on Chapter 1, a "volunteers' index" is not necessary, as the volunteer's DNA profile may be used solely in relation to investigating the specific crime and not entered into the database at all (as is the case in the UK). However, staff elimination databases containing DNA profiles from relevant police officers, medical professionals and laboratory workers, are required, as such persons may contaminate more than one crime scene. See also comments on Clause 28, regarding the merits of creating entirely separate criminal, missing persons' and elimination databases, as different searches are required for each.

Clause 25(2)(a) requires the retention of the "identity of the person" in the case of suspects or offenders, however what this means in practice is not specified. Identifying information is likely to include name but it should be clearly specified what other data might be stored, e.g. physical appearance, address and/or any i.d. numbers. Keeping records of the identities of persons arrested as suspects, even if they are later found to be innocent, is open to abuse: for example people who have merely been arrested (e.g. as the result of a false allegation) could be refused employment or visas on the basis of such records if safeguards to prevent such misuses (including provisions for deletion of records, and limits on access) are not in place. It also remains unclear where information regarding the identity of volunteers (e.g. victims) is to be kept and who is responsible for its security and quality assurance of the link between the case reference number and the relevant crime scene and individual. Is information regarding identities shared with laboratories or do they receive only the case reference number? What information is stored by the police? If identities are shared with laboratories this risks laboratories creating their own mini DNA databases, which may not be secure and could be misused (e.g. to blackmail someone over non-paternity). However, if the identities of victims and others relevant to the case (such as the crime scene examiner) are known only to the police, the police must have the capacity to keep secure, verifiable records and these records must be subject to a process of quality assurance.

Clause 26: does not specify the process to appoint managers of the proposed regional and state databases or how the relationship with the national DNA databank will be managed.

Clause 28(1): More attention needs to be paid to which profiles can be searched against which indices. For example, relatives of missing persons provide their DNA profiles with consent only for

the purpose of finding their missing relative. Their profiles should therefore not be searched for matches with crime scene DNA profiles, otherwise the terms on which they give their consent for their profiles to be stored will have been breached and they may not be willing to provide their samples. In the UK, the missing persons database is now kept entirely separate from the criminal DNA database to avoid this kind of confusion (see response to Clause 2(1)(o) above). Best practice for volunteers' DNA profiles is to use them only for the specific investigation they were provided for and not to search them against all stored crime scene DNA profiles (the best option to achieve this is to remove the proposed volunteers' index altogether, see response to Clause 2(1)(zf and zg)). The UK Police Elimination Database is also a separate database which has specific rules regarding when an officer's DNA profile may be searched against crime scene DNA profiles, in circumstances where he/she may have contaminated evidence. Rules for searching stored elimination profiles from police, medical or laboratory workers in India are currently not specified in the Bill because the need for elimination databases has not been recognised (see comments on Chapter 1). This Clause should also make it clear that experts for both the prosecution and defence are also entitled to access the information provided to law enforcement agencies, tribunals, laboratories and courts by the DNA Database Manager in relation to the case.

Clause 28(2): Information in the missing persons' index (or database, if kept separately), volunteers' index (if retained), unknown deceased persons' index and elimination databases (if set up) etc. should also only be revealed to authorised persons.

Clause 29: This clause fails to limit the purposes for which searches may be performed in responses to requests from foreign governments. In a worst-case scenario this process could reveal the identity and whereabouts of an individual who is wanted by a foreign government for unethical reasons (e.g. an asylum seeker from that country fleeing persecution, or a member of the Indian security services that a foreign service is trying to track down), or reveal the identities and locations of their relatives. This clause should restrict the purposes for which foreign governments may make requests (e.g. to solving serious crimes) and restrict the circumstances in which information will be released, to ensure the human rights of individuals or groups of persons are not compromised.

Clause 29(2) is extraordinarily broad, since the DNA profile of any person identified as a "missing person" or any of their relatives' DNA profiles, can be handed to any foreign government on request, even though such persons are not convicted or even suspected of criminal offences. This clause fails to provide any protection for such persons' privacy or human rights. National security might even be compromised if DNA profiles belonging to the families of politicians or security personnel are sent abroad in this manner. In principle, any DNA profile collected with consent (i.e. from a person who is not convicted or a suspect in the investigation of a relevant serious criminal offence) should only be searched against foreign databases or shared with foreign services with the fully informed consent of the individual (or - in the case of deceased, missing or incapacitated persons - with consent from the relevant family members or guardians).

Clause 30(1): The permanent retention of information from convicted persons may be justified in the case of persons who have committed serious offences. However, if "specified offences" include minor offences, temporary retention of information is more appropriate and consistent with the idea of rehabilitation of offenders. This is particularly the case for children as the retention of their DNA profiles must be consistent with the UN Convention on the Rights of the Child.

Clause 30 (2): This clause is inadequate to implement human rights safeguards in relation to the removal of innocent people's DNA profiles from databases (an issue discussed at length by the European Court of Human Rights[13]). Firstly, it addresses only persons who are acquitted by a court, or who have their conviction overturned, not persons whose cases are dropped before proceeding

to court. Suspects who are arrested but not proceeded against will include the vast majority of innocent persons who are arrested, including many people who may have been the subject of false and malicious accusations: such persons must also have their records deleted when proceedings are dropped. Secondly, the process of awaiting notification from a court is not credible as: (i) there is no requirement for the court to notify the database manager of the outcomes of cases; (ii) no court will in any case be aware of the circumstances of persons whose cases never went to court. Thirdly, reference to the DNA Data Bank Manager suggests that innocent persons' records are to be removed only from the National DNA Databank, whereas innocent people's rights require their records to also be removed from any regional or state databases that are set up under this legislation. This clause should be rewritten to make it unlawful for any DNA Databank to retain innocent persons' DNA profiles. The onus will then be on all DNA Databank managers (national, regional and state) to implement a robust and timely procedure for removals. In the UK, responsibility originally lay with the police to notify the DNA Database Manager when innocent people's DNA profiles should have been removed but an inspection by Her Majesty's Inspectorate of Constabulary (HMIC) revealed in 2000 that at least 50,000 DNA profiles had been retained unlawfully due to failures in the notification process.[14] Rather than sorting out the bureaucratic mess, the then UK Government changed the law to allow innocent people's DNA profiles to be retained indefinitely through legislation that was subsequently found to be unlawful by the European Court of Human Rights. As a result of this judgement, the new Protection of Freedoms Act puts the onus on the DNA database manager to remove those DNA profiles that would otherwise be unlawfully retained: i.e. he or she is obliged to act, not to wait until the necessary information is provided.[15] This has led to a new computer system being implemented to remove innocent people's records from the database automatically.
Provisions for the deletion of children's DNA profiles also need to be included, with some exceptions for those convicted of serious offences.
Individuals should also have a right to know whether their DNA profiles and other personal information is retained, and be able to appeal the retention of their records if they have not been convicted of a specified offence.

Omissions from Chapter V: As noted in the comments on Chapter 1, fully informed consent must be required for the collection of DNA from all persons who are not suspects or convicted offenders, who provide samples on a voluntary basis (e.g victims of crime, relatives of missing persons). The procedure for obtaining consent should be detailed in the text of the Bill. Consent for collection of samples and profiling is separate from consent to retention on a database, and retention and its uses should be appropriately limited. Provisions for withdrawal of consent (leading to the deletion of all records) also need to be included. Further, where the Bill provides for the collection of DNA from some persons without consent (persons suspected of qualified offences) the Bill lacks safeguards to prevent samples being collected merely on the whim of the police, or to prevent persons being arrested simply to obtain their DNA. In most countries, this protection is provided by a legal requirement for a court to issue an order to obtain the suspect's DNA.

### 2.6 Chapter VI: Confidentiality of, and Access to, DNA Profiles, Samples and Records

Clause 33(e) allows a population statistics Data Bank to be set up. However, in the absence of any safeguard to restrict the DNA profile to a forensic DNA profile, based on non-coding DNA (see comment on Clause 2(1)(i)), this clause could lead to health-related research being undertaken without consent, in contravention of the Helsinki Declaration: it is therefore extremely important that this safeguard is introduced. DNA profiles themselves are regarded as "personally identifiable information", since they act as an identifier for an individual and their family, thus the wording of this clause makes little sense. Nevertheless, it is important that statistics can be extracted from the DNA databank to enable proper scrutiny of its achievements (e.g. numbers of criminal investigations

assisted) and shortcomings (e.g. records of adventitious matches, which occur by chance, and whether these occur with related persons) and ideally such claims should be subject to independent academic scrutiny. Approving research uses should be a role for the proposed Ethics and Privacy Regulator (see comments above).

Clause 33(f) should be deleted since civil disputes do not require DNA profiles to be entered on a database and samples can be provided for specific cases from the relevant parties where needed without any use of a database. Allowing the database to be used for civil cases risks a major loss of public trust and serious breaches of privacy e.g. by revealing non-paternity. Instead, the specific roles of identifying missing persons or human remains should be included in the text of the Bill, and Schedule 1 should be deleted.

Clause 33(g) should be deleted. Limiting uses and access is key to providing credible privacy safeguards and maintaining trust, so allowing uses and data-sharing to expand beyond what is specified in the legislation establishing the database is a recipe for loss of public trust. Expanding the extent of sharing without informing volunteers would also breach the basis on which they have consented to provide information to the database.

Clause 34 should be significantly revised: as it stands it allows the DNA Database Manager to open up access to sensitive information with no rationale. This is a major security risk since persons who infiltrate the database could even include criminals who wish to track down victims or identify their relatives, compare DNA profiles to find non-paternity for blackmail purposes, or delete or tamper with records on the database. To minimise this risk, access should be restricted to a small number of paid, trained staff employed by the DNA Database Manager who have been suitably vetted and whose contracts contain confidentiality clauses. This requirement should also extend to regional and state databases. There is no need to access the database for training purposes, since only employed staff need training on how to use the actual database (as opposed to relatively large numbers of people who may require training on collecting or analysing samples, or using DNA evidence in court).

Clause 35. Rather than the loose wording "information obtained from a DNA sample", this clause should use the defined term "DNA profile". Otherwise personal health-related information, or other sensitive genetic information, might be searched. This clause is also too broad in allowing searches that may not be justified, such as searches using DNA profiles from the families of missing persons for purposes other than finding their missing relative.

Clause 36. Access to information in the crime scene index should be restricted to a small number of persons as proposed in the response to Clause 34. Sharing of information with relevant bodies (e.g. a court) is then regulated by Clause 28.

### 2.7 Chapter VII: Finance, Accounts and Audit

Clause 39: For parliament's role in these financial decisions to be meaningful, a financial assessment and cost benefit analysis of the proposed legislation should be provided prior to its scrutiny by parliament. This should include costs of setting up and managing all the proposed/required databases, and estimates of costs of including more or less expansive categories of persons (such as volunteers, or persons suspected of offences for which DNA evidence is unlikely to be relevant). Evidence from the US database shows that obtaining a single crime scene DNA profile is 50 times as effective as obtaining a single offender profile (page 50 of the 2013 report by the Urban Institute[16]). Further, UK evidence shows that collection of DNA on arrest, rather than only from persons charged with an offence, did not increase the number or proportion of crimes detected using DNA, the value of which is mainly driven by the number of crime scene DNA profiles analysed.[17] This is because

most of the value of a DNA database is driven by the systematic retention and searching of crime scene DNA profiles against a limited pool of known suspects for a crime or persons at high risk of re-offending. Therefore, the proponents of the Bill should be required to justify the expansive nature of the provisions to collect DNA from individuals (including from suspects for a wide range of offences and volunteers), rather than prioritising persons previously convicted of serious offences or suspects in cases where a court has identified a DNA sample as important for their trial.

Clause 41: A forward-looking budget plan for the first 5 years should be prepared prior to adoption of the Bill, so that parliament can scrutinise the proposed expenditure. Discrepancies between the budget and the actual spend can then be identified.

Missing provisions: This chapter should also require the Board to publish an annual report containing important public information such as: (i) The number of DNA profiles added to each index (for each database) during the year; (ii) the number of DNA profiles deleted from each index (for each database) and the grounds for the deletions (legal basis); (iii) the number of DNA samples retained and destroyed and their whereabouts (e.g. national, regional, state databases or laboratories); (iv) the number of matches between loaded crime scene DNA profiles and stored individuals' DNA profiles; (v) the number of matches between loaded suspects' and offenders' DNA profiles and stored crime scene DNA profiles; (vi) the number of criminal investigations aided and the proportion leading to a successful prosecution; (vii) number of DNA profiles shared with overseas agencies and the legal basis for these (ix) any other actions taken in relation to provisions in the Bill. The report should be made available for scrutiny by the public and parliament.
The proposed Forensic Science Regulator and Ethics and Privacy Regulator should also publish annual reports and make these publicly available. The minutes of the meetings of the Board and regulators should also be published, to aid public and parliamentary scrutiny.

### 2.8 Chapter VIII: Offences and Penalties

Clauses 45 to 47: The phrase "the DNA bank" should be replaced by "any DNA Bank or forensic laboratory registered under this Act". This is because DNA profiles and samples will be stored at multiple locations, access to any one of which could lead to a breach of an individual's privacy. Note: amendments to Clause 28 must first be made so that lawyers and scientific experts acting for the prosecution or defence in a legal case may access the relevant information.

Clause 49: should refer to a "DNA sample or result thereof, <u>other than their own</u>, in any manner…", since persons are entitled to send their own sample for analysis as they wish and to share the results in any manner they see fit.

Clause 51: In addition to allowing an aggrieved person to approach a court directly (after waiting for 3 months), public trust would be enhanced if such a person could approach a regulator in the first instance, such as the proposed Ethics and Privacy Regulator (in relation to alleged breaches of privacy or other rights), or the proposed Forensic Science Regulator (in relation to alleged technical errors). Then mistakes would likely be rectified more quickly and cheaply than through the courts.

### 2.9 Chapter IX: Miscellaneous

Clause 53: Immunity from prosecution does not sit well with proposed powers to allow the Board and Government to decide who receives access to information and what further indices and uses may be added. If action taken in good faith is to be exempt from prosecution, the actions the Board and Government may take should be more tightly restricted in law (see for example, responses to Clauses 29, 33 f and g, and 34) to make clear that operating outside more tightly specified

restrictions is unlawful. Further, the problems with the provisions for deletion of profiles need to be resolved (see comment on Clause 30(2)), since either the Board or DNA Database Manager(s) need to be made responsible in law for the removal of innocent people's DNA profiles from all relevant databases in a timely way.

Clause 54: It is unclear how or why the Board is expected to make "profits and gains" from operating the database, as the role of the database should limited to solving crimes or identifying missing persons, paid for from government funds. The reference to expectation of profits will increase concerns that other activities are planned which fall outside this remit, such as selling data to private companies.

Clause 55: The existence of this clause reinforces the need for independent regulators (such as the proposed Forensic Science Regulator and Ethics and Privacy Regulator) in addition to a Board, as, whilst the Government is entitled to sack and underperforming database Board, regulators should be independent and not subject to threats of being disbanded.

Clause 56: This clause should be deleted or substantially revised as the Government should only direct the Board to take actions within the remit of the legislation.

Clause 57: gives many powers to Government which should instead be restricted by the Act or given to independent regulators. For example, authorized persons (57(2)b) should be defined in the Act, not subsequently by the Government; 57(2)(c) and (d) should be matters for the proposed Ethics and Privacy Regulator; 57(2)(e) should be deleted since uses should be restricted to those defined in the legislation; 57(2)(f) should be deleted as this should be stated explicitly in a revised Clause (36); 57(2)(k) should be deleted. In particular, allowing Government to define new uses of the DNA database without full parliamentary scrutiny (Clause 57(2)e) creates an unacceptable risk of "mission creep" which will lead to significant mistrust. The phrase "*without prejudice to the generality of the foregoing power*" should also be deleted if the restrictions in the Act are to be meaningful.

Clause 58: gives many powers to the Board which should instead be restricted by the Act or given to other bodies. The phrase "*without prejudice to the generality of the foregoing power*" should be deleted if the restrictions in the Act are to be meaningful. Clauses 58(2)d, e, f, y and z should add "*provided these salaries, allowances and renumerations are consistent with the budgets provided and approved under Chapter VII*". 58(2)(g) should be deleted as the Board should not be allowed to define other purposes not written in the Act and this power under Clause 13 should be deleted, as explained above. Clause 58(2)(j) to (s), and (v), are matters that should be defined by an independent Forensic Science Regulator, as described above. 58(2)(u) should be deleted, as the Board should not have the power to add new indices that are not defined in legislation, as explained above. 58(2)(aa) should be deleted as the Board should not have powers to decide to share other indices with foreign governments beyond what is specified in the Act.

Clauses 60, 62 and 63 should be deleted as they may be used to override individual rights and freedoms, including constitutional rights, privacy rights and information rights. Those drafting the law should instead ensure that it is consistent with existing provisions. Alternatively, they should explicitly seek to amend provisions in existing Acts, where relevant, if parliament accepts that this is justified.

Clause 61 should be deleted as it is not consistent with the rule of law.

### 2.10 Schedule: List of matters of DNA Profiling

This Schedule should be deleted as it concerns the use of the DNA database in cases other than the investigation of "specified offences", as proposed under Clause 33(f), which we propose deleting (see comment above). The specific roles of identifying missing persons or human remains should instead be included in the text of the Bill. The other cases listed here may sometimes involve DNA evidence but this should be collected with consent from the parties involved at the time, not stored on or shared from the DNA database, as this is unnecessary and will create unnecessary risks and loss of public trust.

For example, civil matters should be deleted because samples can be taken specifically for the specified purpose in a given case and not shared more widely. Use of DNA submitted for one purpose (solving a criminal offence) for an entirely different one (e.g. identifying non-paternity) breaches international privacy principles and will lose public trust. Inclusion of such uses is likely to undermine the utility of the DNA database by making people less likely to volunteer to provide their DNA to aid a criminal investigation or find a missing person.

**For further information contact:**

Dr Helen Wallace
Director
GeneWatch UK
60 Lightwood Rd
Buxton
SK17 7BB
Tel: +44-1298-24300
Email: helen.wallace@genewatch.org
Website: www.genewatch.org

[1] http://dnapolicyinitiative.org/

[2] http://dnapolicyinitiative.org/wiki/index.php?title=Main_Page

[3] Council for Responsible Genetics: Overview and Concerns Regarding the Indian Draft DNA Profiling Act. April 2012.
http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/India_DNA_Bill_Memo_2.0.pdf

[4] Crown Prosecution Service: Guidance on DNA Charging. 16th July 2004.
https://www.cps.gov.uk/legal/assets/uploads/files/pdf_000328%20-%20%20DNA%20Charging%20Guidance.pdf

[5] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland.
http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf

[6] UK Home Office (2013) Biennial report 2009 to 2011: National DNA Database.
https://www.gov.uk/government/publications/ndnad-biennial-report-2009-to-2011

[7] THE FIRST SCHEDULE: CLASSIFICATION OF OFFENCES.
http://ecourts.gov.in/sites/default/files/classification.pdf

[8] NDNAD Ethics Group: annual report 2008.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118889/NDNAD_Ethics_Group_Annual_Report.pdf

[9] UK Home Office (2013) Biennial report 2009 to 2011: National DNA Database.
https://www.gov.uk/government/publications/ndnad-biennial-report-2009-to-2011

[10] UK Forensic Science Regulator (2014). Protocol: DNA contamination detection – The management and use of staff elimination DNA databases. FSR-P-302. ISSUE 1.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/355995/DNAcontaminationDetection.pdf

[11] https://www.gov.uk/government/organisations/forensic-science-regulator
[12] UK Forensic Science Regulator (2015) The control and avoidance of contamination in crime scene examination involving DNA evidence recovery: draft guidance. FSR-G-206. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/393866/206_FSR_SOC_contamination_consultation.pdf
[13] European Court of Human Rights. Grand Chamber. CASE OF S. AND MARPER v. THE UNITED KINGDOM. JUDGMENT STRASBOURG 4th December 2008. http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20EN.pdf
[14] Her Majesty's Inspectorate of Constabulary (2000). Under the Microscope: Thematic Inspection Report on Scientific and Technical Support. London, Home Office.
[15] Protection of Freedoms Act 2012. http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
[16] Collecting DNA at arrest: Policies, practices and implications. The Urban Institute. May 2013. https://www.ncjrs.gov/pdffiles1/nij/grants/242812.pdf
[17] Wallace HM, Jackson AR, Gruber J & Thibedeau AD (2014). Forensic DNA databases - Ethical and legal standards: A global review. *Egyptian Journal of Forensic Sciences*, **4**(3), 57–63. http://www.sciencedirect.com/science/article/pii/S2090536X14000239