

Forensic use of bioinformation: ethical issues

Nuffield Council on Bioethics

Introductory remarks

The responses to these questions have been drawn from a report shortly to be published by The Royal Academy of Engineering entitled 'Dilemmas of Privacy and Surveillance', and from considerations by the Academy's Ethics working group. The report, to be published in spring 2007, considers the role of technology in the increasing levels of surveillance and the amount of personal data collected about individuals. The report considers the impacts of this increased data collection and gives recommendations for the development and management of technologies in a way that protects privacy.

The main thrust of the responses below is that DNA samples and profiles should be collected only when there is good reason and, in the case of samples taken from volunteers, where there is explicit consent for the samples to be used for a given purpose. Samples and profiles should also only be retained when there is good reason or explicit consent – they should not be kept on the basis of the existence of a mere possibility of their being useful in detecting future crimes. If a volunteer offers to give a sample to help the investigation of a specified crime, this consent cannot be extended to the investigation of other crimes, past present or future, or other purposes.

A reason for this stance is due to the particular nature of DNA profiles. They are useful not only for identifying suspects in a crime, but can be used to identify family relationships and predict future disease. Therefore, DNA profiles constitute sensitive personal information. However, many of the points also apply to other biometric information such as fingerprints and facial images, the retention of which raises privacy-sensitive issues. It is essential that the drive to prevent or detect crime does not result in an infringement of the privacy of innocent civilians.

1. The interpretation of bioinformation

- a. *In your view, is the SGM Plus system, which uses ten STR markers, sufficiently reliable for use in ascertaining the identity of suspects in criminal investigations and/or criminal trials?*

The Royal Academy of Engineering can offer no opinion on whether the statistics presented for the accuracy of the SGM Plus system are correct. However, assuming they are correct, those statistics do suggest that it is extremely reliable, with instances of failure very rare. Therefore, the evidence that the system produces is of value in ascertaining the identity of suspects in criminal trials. However, it is important that the rarity of failures does not give the impression that the system *cannot* fail. It is not impossible that the system could falsely match an individual with bioinformation found at a crime scene, especially if that individual is related to the true source of that bioinformation. This should always be made clear when DNA evidence is presented.

As long as there is room for improvement in the reliability of the current system those improvements should be made, provided that the cost of using a more sophisticated system is not excessive. However, even a perfectly accurate system will not differentiate between traces of bioinformation left at a crime scene by the perpetrator of a crime and traces that may have been planted at the scene – such as cigarette butts or other items which could carry traces of DNA. Therefore, further evidence supporting an individual's presence at a crime scene will always be necessary.

2. Sampling powers

- a. *From whom should the police be able to take fingerprints and DNA samples? At what stages in criminal investigations and for what purposes? Should the police be able to request further information from DNA analysts, such as physical characteristics or ethnic inferences?*

Current law states that fingerprints and DNA samples can be taken from any suspect in a crime, and it is generally acceptable to collect bioinformation when the elimination of suspects is essential to the investigation of a crime.

However, it is questionable whether law should allow fingerprints and DNA to be taken in a minor incident to which forensic evidence is irrelevant. Samples should not be taken in such circumstance simply to be used in a speculative search against a database of unsolved crimes. Such searches should only be carried out when there is reason to believe that an individual has been involved in previous criminal activity; for example when the nature of the crime suggests that it is part of a pattern of behaviour, or the suspect matches a description of a suspect from a previous crime.

The unreliable nature of drawing physical characteristics or ethnic inferences from DNA evidence means that DNA analysts should not be asked for such information. If such information it is likely to mislead, it will hinder rather than help an inquiry.

- b. *Should police expenditure on bioinformation collection and analysis be given priority over other budgetary demands?*

It should not; on the basis that bioinformation should not be used as evidence in isolation from other evidence. Bioinformation should not be treated as the one and only way to investigate crimes and bring them to trial. Moreover, it is important that a significant proportion of the police budget be dedicated to crime prevention alongside investigation.

- c. *Do you consider the current criteria for the collection of bioinformation to be proportionate to the aims of preventing, investigating, detecting and prosecuting criminal offences? In particular: is the retention of bioinformation from those who are not convicted of an offence proportionate to the needs of law enforcement?*

The Bichard inquiry arising from the Soham murders focussed on the importance of the retention and sharing of police records in order to prevent crimes. In the Soham case, Humberside police had information about Ian Huntley and his relationships with underage girls which should have been kept and shared with other police forces. Although Huntley had no convictions when he moved to Soham, the intelligence that the police held about him was serious enough to warrant sharing with the police in Cambridgeshire. Therefore, there is good reason for arguing that even when an individual is not convicted of a crime, information about them should be stored and shared if that information is of a serious nature.

However, to a large extent the information that needs to be shared will be information relating to convictions, allegations made against a person and other police intelligence rather than bioinformation as such. Sharing intelligence is useful in preventing crimes, bioinformation less so.

In cases where the intelligence suggests potential involvement in future or past crimes, bioinformation *could* be taken and retained even where there is no conviction, and should be held nationally along with the relevant intelligence. These will be cases such as that of Huntley, where offences had been committed, but for some reason had not resulted in a prosecution. In such cases there is justification for believing that the bioinformation may be useful in future investigations.

However, where no such intelligence and therefore no such justification exists, collecting and retaining the bioinformation of individuals convicted of no offence is not proportionate to the needs of law enforcement. If a person is not deemed to have committed an offence then there is no use for the bioinformation in investigating a particular offence. If there is no reason for assuming that the person has committed crimes before or is likely to do so in the future, there will be no investigative use for that bioinformation.

It may well be the case that retained DNA profiles are subsequently matched with scene of crime samples but, given that often police have other leads on the identity of a suspect before a match is made (in 42% of cases according to this consultation paper), the justification for this is somewhat diminished.

Retaining DNA profiles without specific reason and justification is problematic because it increases the risk of 'function creep': using data for purposes other than those for which it was originally intended. Function creep seems to be a threat in cases where bioinformation is kept purely on the basis that it may have some use in the future.

- d. *Is it acceptable for bioinformation to be taken from minors and for their DNA profiles to be put on the NDNAD?*

The Royal Academy of engineering has no comment to make on the specific case of minors in the criminal justice system.

3. The management of the NDNAD

- a. *Is it proportionate for bioinformation from i) suspects and ii) volunteers to be kept on forensic databases indefinitely? Should criminal justice and elimination samples also be kept indefinitely? How should the discretion of Chief Constables to remove profiles and samples from the NDNAD be exercised and overseen?*

Whether suspects' data should be kept on databases indefinitely depends on whether they go on to be convicted and on the nature of their crime. If someone is convicted of a crime, if that is a minor offence, an offence of a nature that is unlikely to lead to escalation, or an offence in which DNA evidence is unlikely to be of use (eg, fraud), then there is no clear justification for retaining their DNA data. However, if a pattern of behaviour, or other police intelligence, suggests that further offences are likely then there is reason for retaining the samples (see answer 2c.). These reasons should be clearly stated, and should be open to challenge.

It is neither appropriate nor proportionate to keep volunteers' data on forensic databases indefinitely. Volunteers agree to offer DNA samples to aid the detection of a specific crime and they do not expect that in doing so they are giving consent for their DNA profiles to be used for an open-ended range of purposes. Furthermore, it is unclear how storing bioinformation from such individuals is useful for preventing, detecting or prosecuting a crime since people who volunteer samples will more likely

be those who have not been involved in crime. If individuals are asked to volunteer samples of DNA to be kept on a databases for an indefinite period to be used in numerous future crimes, this is likely to deter individuals from volunteering samples.

In terms of removing profiles and samples from the NDNAD it would be more appropriate if this did not depend on the discretion of a Chief Constable. There should be clear, universal guidelines on this topic and it would be preferable for the decision to be handed over to the NDNAD Custodian unit, or an independent body with a specific remit to oversee the collection, retention and use of forensic bioinformation (a body akin to the HFEA). The Custodian, or independent agency, could weigh objectively the policing case for retaining the data and the arguments for removing it from the database.

- b. *Is the ethical oversight of the NDNAD adequate? What, if any, research on NDNAD profiles or samples should be permitted? Who should be involved in the oversight of such databases and granting permission to use forensic DNA profiles of samples for research?*

The fact that the use of the NDNAD is governed by the Data Protection Act 1998 (DPA) means that it is not adequately governed. The principles of good data processing in the DPA are relevant to, and should apply to, the NDNAD, but the DPA has exceptions and exemptions for data used in the prevention and investigations of crimes and in legal proceedings. This means that its principles will not cover many of the uses of the NDNAD. There needs to be new legislation or an extension of the DPA to cover databases such as the NDNAD, the uses of which are often exempted from the DPA.

Non-forensic research on NDNAD profiles or samples should not be permitted. Even if a person is convicted of a criminal offence, they do not lose the right to withhold consent to being involved in research. Using the samples and profiles in this way constitutes involving them in research without their consent.

- c. *Who should have access to information on the NDNAD and IDENT1 databases and how should such information be protected from unauthorised uses and users? Should forensic databases ever be made available for non-criminal investigations, such as parental searches or identification of missing or deceased persons?*

Both of these databases should be used only for very specific purposes and access to the databases should be carefully monitored. There must be clear, universal guidelines concerning access to the databases, and stringent selection and training of those staff who will access the database.

It is extremely difficult to protect such databases from unauthorised users and usage. The main strategies for protecting databases is to ensure that any data stored on them is stored in an encrypted form, to ensure that only relevant data is stored and to ensure that the data is held for as short a time as is necessary. These principles of course count against data being retained on the NDNAD indefinitely, especially in the case of individuals who have not been convicted of any criminal offence.

The use of the database for non-criminal investigations should be carefully limited. There is a case for using the database for the identification of missing and deceased persons, when other avenues for so doing have been exhausted. It is important not to use it for this purpose as a matter of course, as this might create a motivation for enlarging the database.

The use of such databases for parental searches should not be allowed. This is a very sensitive issue that would affect more than the individual who is on the database, but also their extended family. There is no justification for intruding on the privacy of members of the extended family who do not appear on the database.

- d. *What issues are raised by the transfer of bioinformation between agencies and countries? How should such transfers be facilitated and what safeguards should be in place for the storage and use of transferred data?*

There is already some sharing of information on the database between government agencies, with access to the database strictly controlled. However, the transfer of data increases the risk of it being accessed by unauthorised persons and misused. Therefore data should only be transferred in those circumstances in which it is strictly necessary. Transferred data should be encrypted to prevent it being misused if it reaches the wrong hands. It should always be stored in an encrypted form. Staff from other agencies who will access the data should undergo stringent selection and training.

4. Ethical issues

- a. *Is the use of DNA profiles in 'familial searching' inquiries proportionate to the needs of criminal investigations? Do you consider the use of familial searching to be an unwarranted invasion of family privacy?*

The use of familial searching does constitute an unwarranted invasion of family privacy. Involving the innocent relatives of a suspect in a criminal investigation could cause unnecessary upset and distress. Family relationships are often complex, with some relationships unknown or broken down. Therefore, involving relatives of a suspect in an investigation could cause great harm to a family.

In some cases, where a crime is particularly serious, the use of familial searching might be proportionate. However, given the potentially harmful consequences noted above, the circumstances in which familial searching is carried out should be limited.

- b. *Certain groups, such as ethnic minorities and young males, are disproportionately represented on forensic databases. Is the potential for bias within these databases acceptable?*

The potential for bias in the databases is not acceptable. However, the issue in this case is why some groups are disproportionately represented. It may be that this is due to the circumstances in which DNA samples are taken. If it is the case that some groups are more likely to come under police suspicion (either because they are more likely to be identified as suspects in a crime or they are more likely to be arrested for their behaviour) and are for this reason more likely to appear on the database, then it is this underlying bias that needs to be addressed. Of course, a forensic database is unlikely to represent an accurate cross-section of the UK population but, if there is significant distortion in the database, then the reasons for the arrests which lead to the collection of samples need to be scrutinised.

- c. *Is it acceptable that volunteers (such as victims, witnesses, mass screen volunteers) also have their profiles retained on the NDNAD? Should consent be irrevocable for individuals who agree initially to the retention of samples voluntarily given to the police? Are the provisions for obtaining consent*

appropriate? Should volunteers be able to withdraw their consent at a later stage?

Volunteers' profiles should not be retained on the NDNAD after the case to which they relate is closed. Volunteers offer samples in order to assist with a particular inquiry and their consent for their samples and profiles to be used in that case cannot be extended to further cases.

Consent to the retention of samples and profiles should not be irrevocable and individuals should be able to request that their profiles be removed from the database. This is because, as the technologies develop, the use of the NDNAD may change, and an individual may as a result no longer feel comfortable with their samples and profiles being on the database.

In addition to the fraught nature of the circumstances in which DNA samples will be taken, the complexity of the nature of DNA profiling and analysis makes informed consent very difficult. Most individuals will not fully appreciate how their bioinformation could be used, the likelihood of mismatches of samples with the NDNAD and so on. For this reason they should be able to revoke consent if further reflection or learning about the issue causes them concern. It may be useful to allow a 'cooling off' period in which people can easily revoke consent so that profiles are not added to the database straightaway and can be destroyed if the subject so wishes.

A possible solution would be to take samples from volunteers for the purposes of the investigation, but not to seek consent for those samples to be retained at the moment they are collected. Rather, once the investigation is closed, volunteers could be contacted to ask whether they consent to their samples being retained. Active consent should be sought at this stage: volunteers actively agreeing to retention, rather than having to actively deny consent.

- d. *Would the collection of DNA from everyone at birth be more equitable than collecting samples from only those who come into contact with the criminal justice system? Would the establishment of such a population-wide forensic database be proportionate to the needs of law enforcement? What are the arguments for and against an extension of the database?*

Although universal representation on a database will mean proportionate representation of every social group, this does not mean that a universal database would be fair. Presence on the database potentially involves a person in the investigation of any crime. It is therefore arguable that it is fairer for the database only to extend to those who have been convicted of, or are suspects in, a crime.

It would not only therefore be inequitable, but it would be wholly disproportionate to the needs of law enforcement for the database to be populated by millions of individuals who will have no contact with the criminal justice system. It is in fact likely that a vast bank of data will actually hamper criminal investigations, as there will be more data to sift through when searching for suspects, much of which will be irrelevant. This will be complicated by the fact that, the more profiles are present on the database, the more likely it is that mismatches will occur. Furthermore, since people leave traces of bioinformation wherever they go, it is also likely that many more innocent people will come under suspicion if their bioinformation is found at the scene of a crime, since a comprehensive database would mean that they were automatically identified. Therefore, a totally comprehensive database could in fact

make criminal investigations more difficult and could cause unwarranted distress to innocent individuals.

It is also unacceptable to treat all members of a society as potential suspects in a crime, as inclusion in the database would.

5. The evidential value of bioinformation

- a. *What should be done to ensure that police, legal professionals, witnesses and jury members have sufficient understanding of any forensic bioinformation relevant to their participation in the criminal justice system?*

The crucial issue is that those involved in the criminal justice system understand the statistical likelihood of DNA evidence being correct or incorrect. In order to ensure that this is the case, the statistical evidence needs to be presented as clearly as possible in a number of ways, in order that it is appreciated. One means for aiding this is to have a statistics expert explain to a court the likelihood that evidence based on DNA could be mistaken, as well as the forensic scientist who has analysed the DNA data. Ideally, courts would have access to a science communicator, able to explain in everyday language the significance of the evidence and the meaning of the statistics involved. A jury will not be able to become proficient in biochemistry but can be helped to grasp the statistical probability of a procedure's failure. If that explanation comes from an independent expert rather than the scientist who has presented the DNA evidence, this might help to counteract the persuasive power of the scientific evidence.

- b. *How much other evidence should be required before a defendant can be convicted in a case with a declared DNA match? Should a DNA match ever be taken to be sufficient to prove guilt in the absence of other evidence?*

A DNA match, on its own, should never be treated as sufficient to prove guilt. The difficulty of ensuring that the relative significance of DNA evidence is appreciated is good reason for it to be presented alongside other evidence.

As discussed above, although false matches are statistically unlikely, they are not impossible, so further evidence is needed to corroborate the match. Furthermore, it is possible to plant DNA at the scene of a crime, with the developments in technologies for synthesising DNA offering increasing means of doing this. Therefore, there must be further evidence to support the claim that a suspect was at the scene of a crime to rule out this possibility. How much further evidence is sufficient to prove guilt will depend on the circumstances, and this would be for a jury to decide.

6. Other issues

- a. Are there other issues, within our terms of reference, which we should consider?

An issue that may be worthy of consideration is the potential impact on forensics of collecting biometric data for the purposes of identification, as has been suggested for the national ID cards programme. If, for example, fingerprints are to be taken from every citizen of a country to be recorded on their ID cards, could and should these be used in detecting crimes? Would it be acceptable to use other biometrics used for verification of identity in criminal investigations? The move towards data sharing suggests that this could be a possibility. However, for the reasons given above

against the existence of a comprehensive DNA database, this would not be an acceptable situation.

Submitted by:

Mr Philip Greenish CBE
Chief Executive
The Royal Academy of Engineering

Prepared by:

Dr Natasha McCarthy
Policy Advisor
30th January 2007