

Nuffield Council on Bioethics

Note of a Workshop on the use of person-specific biological information for legal, forensic and police purposes

Tuesday 21 February 2006

28 Bedford Square, London, WC1B 3JS

Present: Dr Bob Bramley
Dr Jonathan Cave
Dr John Daugman
Professor John Dupré
Mrs Lyn Fereday
Mr Tony Lake
Professor Graeme Laurie
Dr Eric Metcalfe
Dr Bronwyn Parry
Professor Maxime Seligmann
Dr Alaster Smith
Professor John Spencer
Maître Mario Stasi
Professor Sir John Sulston
Mr Robin Williams

Professor Sir Bob Hepple, QC, FBA (Chairman)
Professor Roger Brownsword
Professor Margot Brazier
Professor Peter Lipton
Dr Alan Williamson

Professor Sandy Thomas
Mr Harald Schmidt
Ms Catherine Joynson
Ms Caroline Rogers
Mrs Julia Trusler

- 1 The Chairman welcomed the delegates and noted that the Workshop aimed to provide a forum for identifying and discussing ethical, legal and social issues raised by current and potential forensic uses of biological information. Discussion of the National DNA Database and its expansion over the last few years formed a major part of the Workshop. Other emerging technologies, especially biometrics, were also considered within the more general context of a decline in personal privacy over the past decade. Mobile telephone records which can track the location of

individuals, and increasing CCTV coverage have contributed to this decline. Conclusions from the discussions would inform any future investigation of the topic by the Council.

The National DNA Database

- 2 In the first presentation, the National DNA Database (NDNAD) was described as a valuable asset in identifying perpetrators of crimes. Biological samples were taken at the discretion of the police, with or without consent, from people who had been arrested for a recordable offence. Samples were also taken from volunteers and from crime scenes. The samples were subsequently stored by freezing. The markers were generated from short sequences of DNA, called short tandem repeat (STR) sequences, derived from non-coding regions of different chromosomes. Each sample was used to generate a profile from measurements at ten loci and a sex marker. As far as it was known, the profiles did not allow any information on a person's health or other characteristics, other than gender, to be determined. It took a matter of seconds to check a new profile against those already stored on the database.
- 3 The NDNAD was the largest DNA intelligence database in the world. It contained profiles from 3.2 million different individuals, accounting for over 5% of the total population and 8-9% of the male population. A disproportionate number was from young males, a reflection of the 2003 Crime and Justice Survey which showed that males aged between 10 and 25 accounted for almost half of all offences committed. Young black men in particular were highly represented on the database. In the following discussion the view was expressed that many young males 'grew out' of crime. The database was not a 'criminal database', however, as it included 13-14,000 profiles from volunteers and profiles from some 180,000 people who had either not been prosecuted for a criminal offence or who had been acquitted. In addition to the profiles of samples taken from people, the NDNAD included 200,000 samples taken from crime scenes. These were usually removed from the database following a match with a suspect.
- 4 The volunteers on the database would usually have consented to give a sample for elimination purposes in relation to a specific investigation, but the profiles obtained were not added to the NDNAD unless the volunteers had given separate written consent for this. Such consent, once given, was irrevocable in England and Wales, but not in Scotland. Voluntary samples were not taken from children without consent from an adult with appropriate responsibility.

- 5 It was observed that the value of having a database of subjects who had been arrested for any recordable offence was that 80% of the matches obtained involved offences different from the initial arrest offence. The longevity of some criminal careers and the progressive nature of criminal behaviour resulted in the identification of some suspects for serious crimes directly as result of their being arrested for a lesser offence and their profile matching that from the serious crime.
- 6 At first it was thought that the NDNAD would only be used to find the perpetrators of the most serious crimes and the police used it successfully in a large number of cases. It had been particularly helpful in solving 'cold cases' where renewed investigation was possible because of developments in technology that enabled forensic scientists to make use of heavily degraded DNA. However, its impact had been much wider and most matches now identified suspects for 'volume' crimes, such as burglary and theft. This had resulted in the detection rate for domestic burglary, for example, being 41% where DNA evidence was available compared with 16% when it was absent.
- 7 Approximately 900 database matches between subject and crime scene samples were reported each week, and when a new crime scene profile was loaded onto the database, there was a 55% chance of obtaining an immediate match with an existing subject's profile.
- 8 It emerged in discussion, however, that DNA profiles were loaded onto the NDNAD for only about 1% of all recorded crimes. This was in part due to DNA samples being inapplicable in many areas, such as 'white collar' crime, and in part due to practical difficulties in locating and recovering DNA evidence where it was available. So the overall impact on the crime detection figures was less than might be expected.

Oversight and custodianship of the NDNAD

- 9 The Custodian of the NDNAD was accountable to the NDNAD Strategy Board for setting the standards, protocols and procedures for suppliers of profiles to the Database, monitoring suppliers for compliance, management and security of the NDNAD, the provision of operational services from the NDNAD, and advising the Board on scientific matters. The NDNAD Strategy Board was responsible for policy development, strategic management and oversight of the Custodian. A Commissioner from the Human Genetic Commission (HGC) had been a member of the Board for several years and the HGC had recently been asked to nominate a second representative to join it. Steps were currently being taken to establish an ethics committee and there seemed to be a general agreement at the Workshop that this was a good development.

Retention of profiles and samples from those not convicted of offences

- 10 Much of the discussion focused on the changes to the law in 2001 that allowed the police in England and Wales to retain on the NDNAD the profiles of people who had been charged with a recordable offence but not later prosecuted or convicted, and in 2003 when revised legislation extended retention powers to include samples of all of those arrested for a recordable offence. These profiles would previously had to have been removed and not been available to rapidly identify recidivists. Since the law changed in 2001, nearly 9,000 suspects had been identified among the 180,000 persons whose profiles had so been retained by matching them with profiles from samples from crime scenes.
- 11 The Chief Constable of the relevant Police Force had the right to decide whether or not to remove an individual arrestee's sample from the database. To ensure consistency of approach, the police were currently drawing up guidance as to the circumstances where this discretion should be applied, although it was stressed that the circumstances would have to be 'exceptional', where no crime had been committed for example.
- 12 The Police and Criminal Evidence Act (PACE) describes the circumstances in which non-intimate samples may be taken from a person in police detention following their arrest for a recordable offence. PACE does not differentiate between adults and juveniles in this particular area. It was noted that the Home Office had recently confirmed that the profiles of minors whether convicted of a crime or not; were also retained on the database.
- 13 The progressive expansion of the NDNAD was a concern to some delegates, and more widely in the population, due to its perceived discriminatory nature and reduction of individual liberty. Samples from the same small proportion of the population would be continuously used to search for a match from a crime scene and there was concern that the system was therefore blind to new entrants and did not protect citizens equally from mistakes. Juries might also presume that because a suspect's profile was on the NDNAD she or he was more likely to be guilty of the current offence. The Home Office representatives pointed out that all crime scene profiles were checked continuously for matches as new subject profiles were added to the database and that the courts were not informed that accused persons had been identified because their profile was on the NDNAD. Even if they were it did not mean that they had a previous record as the database was not a 'criminal' database. There was much to be done to change public perception that the NDNAD was a database of criminals and to address the other concerns.
- 14 Delegates suggested that a database of samples from three million people at random might be no less effective than the current database. The police personnel present, however, drew attention to the fact that a large

proportion of crime was committed by a small number of people and it was better to focus attention on these.

- 15 It was further suggested that some judges believed that the solution to overcome concerns over the retention of profiles on the NDNAD from innocent people or those who had not been convicted was to create a DNA database that included every member of the population. In response, the Home Office delegate reported that there was no intention to increase the NDNAD in this way as it was not perceived to be proportionate to the probability of identifying criminals.

Familial searching

- 16 The NDNAD was used in a particular way for 'familial searching', whereby a crime scene profile that had no exact matches with a subject's profile on the database was checked for matches with profiles that could have come from a parent, child or sibling of the offender. This type of search could generate a large list of suspects which would typically be reduced by carrying out further enquiries to establish if they could actually be a true relative of the offender and/or carrying out further tests on the crime scene sample and stored subject samples, using Y-STR and mitochondrial DNA testing for example.
- 17 It was recognised by the NDNAD Strategy Board from the outset that this type of search would be of a very sensitive kind, as it could reveal previously unknown or undisclosed information, such as non-parentage. There was also the possibility that the person originally matched on the NDNAD might feel responsible for the identification of the suspect. The NDNAD Strategy Board sought advice from its HGC representative and the Information Commissioner before endorsing the approach. In line with the advice received familial searching has been approved for use only in the most serious offences and a Good Practice Guide has been produced for how to follow through the investigation. In the following discussion the view was taken that even if this type of searching of the NDNAD was carried out in a sensitive way, over time there might be a risk that the procedures become routine and thus not be carried out as carefully.

Storage and use of samples

- 18 Storage of the samples in addition to a limited profile of markers was a concern for some people, as significantly more information than required for simply identification purposes could be revealed by further analysis. There was also concern that its scope could be expanded through development of new technologies and that the current limitations on use of the database could change in the future under the oversight of new political administrations. Additionally, if the NDNAD were to be used internationally, other governments might have different controls.

- 19 Representatives from the Home Office explained that the samples were retained primarily to allow the profiles on the database to be upgraded as new technologies were introduced, for example to increase the number of markers in each profile and thus reduce the risk of two profiles matching just by chance. Such upgrading had already happened once. Between 1995 and 1999, six sequence pairs had been used for the database, giving a match probability of 1/50 million. This would have provided an insufficient level of discrimination as the database continued to grow in size, so the number of markers was increased to ten pairs, giving a match probability of 1/1 billion or lower. No chance matches have yet been confirmed at this level of discriminating power. However, rather than upgrade the whole database to the new marker system, if a sample from a match involves a profile with only six markers (taken before 1999) the stored sample is retrieved and verified for ten markers. A further increase in the number and type of markers that form a profile is likely to be needed in the future to enable improved profiling of degraded DNA samples from crime scenes and to provide for even greater discriminating power as international use of DNA databases was expected to expand.
- 20 It was reported that there was already increasing international use of DNA databases.¹ Further developments were also under consideration by the European Union and more widely following the publication by the European Commission of the *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. If adopted, this would ensure that Member States allowed the disclosure of personal data to the competent authorities of other Member States for the purposes of police and judicial cooperation, although the law pertaining in each Member State would remain paramount when deciding when, what and to whom information from the database would be provided.

Other uses of the NDNAD

- 21 Until 2005, the NDNAD could only be used for purposes relating to the prevention and detection of crime. When permission to use the database in the identification of victims of the Asian Tsunami was requested, it was originally refused as the request was not in connection to a suspected crime. However, changes had subsequently been made such that the NDNAD could now be used to identify a deceased person or body part in such circumstances.
- 22 As regards the use of the data on the NDNAD for research, the samples and data can only be used for purposes related to the prevention and

¹ It was noted that no personal data was shared via DNA databases, but just a unique identifying number and the DNA profile which, with the exception of the sex marker, contained no genetic information.

detection of crime. This could extend to research on crime, criminals and tracing offenders. However, the NDNAD Strategy Board would need to be approached for permission in each case. The Board would need to be convinced of the legality and usefulness of the proposed research and would take advice on the ethics of the proposal. It was reported that this is where the Board's proposal for an ethics committee would have greatest value. To date the NDNAD Strategy Board had received 34 requests for research and approximately ten had been granted.

- 23 Delegates commented that research could potentially reveal physical characteristics that could be identified from a genetic sample found at a crime scene. The Home Office said that techniques to indicate hair and eye colour were already available, but this type of information was not stored on the database and was only indicative. It was agreed that there were a large number of genes involved in physical appearance and it would be unlikely that a 'genetic photofit' could be produced.

Legal and human rights issues

- 24 In the UK the status and functions of biometric databases (except the NDNAD) were governed under the general law, rather than on a specific statutory basis as was the case in certain other countries, such as France. Personal information and samples were protected in the UK by the Data Protection Act 1998 and the Human Tissue Act 2004. However, both of these pieces of legislation contained exceptions that allowed the police to access personal data and samples for the purposes of investigating crime.
- 25 The Human Rights Act 1998 incorporated the European Convention on Human Rights into UK national law. Acts of Parliament were now required to comply with the Human Rights Act. Article 8 of this Act provided for everyone to have "the right to respect for his private and family life, his home and his correspondence". In this case, however, there was a clear exemption that allowed interference with the exercise of this right by a public authority "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".
- 26 It was observed that the authorities in the UK had, in recent years, carried out certain activities that could be perceived as impinging on civil liberties. A recent case² heard in the House of Lords had tested whether the storage of biometric information on the NDNAD from two individuals who

² In the case of *S and Marper*, 4 out of 5 Law Lords found there was no interference with Article 8(1) of the ECHR. The other one found that there was some interference but that it was proportionate and justified under Article 8(2). The Law Lords also found there was no interference under Article 14 (the right to non discrimination).

were not convicted of any crime was covered by Article 8. The Lords concluded that the mere storage (as against the dissemination) of private information was potentially within its scope whereas the storage of DNA that would enable only identification (but not enable other information about a person to be gleaned from it) was not. However, even if the storage of DNA samples fell under the scope of Article 8, the purposes of law enforcement for which the samples in this particular case were stored amounted to a justification. One of the individuals was a minor who had been arrested for robbery and one was an adult male who had been arrested and charged for harassment of his partner. The former was acquitted and court proceedings for the latter were discontinued after his partner decided not to press the charge.³

Generation Scotland: a database for use in medical research

- 27 Generation Scotland was a project that was established with the aim of providing data for use in identifying the genetic basis of common complex diseases. The project was intended to follow the health of 50,000 individuals in Scotland, collecting information on environmental and lifestyle factors at the outset and linking this to medical records and results from tests on biological samples.
- 28 The founders of Generation Scotland recognised that maintaining public confidence was very important for the success of the project. An oversight process called 'regulation plus' had been developed to ensure that the standards that had been set out were met. Exercises in public engagement had been held, and the results used to develop the consent form and the information provided to participants.
- 29 Recruitment of volunteers aged 35–55 was due to start in 2006 through general practitioners. Volunteers would be asked to invite their close relatives to take part. Ideally, groups of three siblings would be recruited. In this way, fewer people overall would be needed to achieve the same statistical power than if unrelated individuals were used.
- 30 Lifestyle information, cognitive tests, blood samples and access to medical records would be requested from volunteers. If people wished to participate they would be required to consent to all of these processes. If an individual wished to withdraw from the project at a later stage s/he could do so in different ways: complete withdrawal, whereby researchers would guarantee to remove the samples and electronic information as far as possible; and discontinued participation, whereby the participant would allow researchers to use data already included in the project with the

³ Regina v. Chief Constable of South Yorkshire Police [2004] 1 WLR 2196.

option of continuing to allow access to his/her medical record but without further direct contact.

- 31 There was the possibility that Generation Scotland would receive requests from the police to use data or databases generated by the project, although these were expected to be very infrequent. The legal system allowed access by the police given by a court order which would only be granted for a specific investigation into serious crime. However it was reported that 'serious crime' has a broad definition in Scottish law. Opinion polls have revealed conflicting results with regard to the question of whether or not the police should have access to databases of biological information intended for medical research. The Generation Scotland project team has announced that it was strongly against police access as recruitment and participation could be adversely affected. It might also introduce a sampling bias in the kind of the people who volunteered or conversely, did not wish to participate. The organisers of Generation Scotland had stated that they would make representations to the court strongly opposing such an order in all circumstances. It had been decided that specific information about these issues should be provided in leaflets for potential participants about the project.

Biometric technology

Current iris scanning technologies

- 32 The discussion of this topic commenced with a presentation considering 'what is currently biometrically possible'. A study of 200 billion iris cross-comparisons had shown that reliable biometric identification, including all-to-all comparisons (matching each biometric profile to every other) was technologically possible. The results of this study were used to determine false-match rates and matching thresholds suitable for one-to-one and all-to-all comparisons.
- 33 Iris-scanning biometric technology was currently used in various contexts around the world. These included at airports for check-in, security clearance, immigration control, as a substitute for passport inspection, and to control access of employees or residents to specific buildings, rooms or areas. An example was presented in which the technology had been used by a methadone clinic to verify that the correct person was receiving treatment and also to ensure that the appropriate quantity of medication was administered.
- 34 The border protection iris database of the United Arab Emirates was one of the largest. This programme was launched in 2001 to compare the iris patterns of foreign visitors with those on 'watch lists' of people expelled from the country. Iris patterns from over 300,000 people were held on the watch list, and on a typical day 12,000 irises were compared to those

on the database. This totalled seven billion comparisons per day, with each search taking less than two seconds. So far a total of two trillion iris comparisons have been performed and around 40,000 people have been caught trying to enter the country with false travel documents.

Advantages and limitations of iris scanning

- 35 Certain properties of the eye gave iris scanning a number of advantages as a biometric technology, including high levels of randomness and complexity, and long-term stability. Indeed, iris codes typically contained 2,048 data bits from each iris, of which around 250 bits were independent; this compares to 20 metrics for facial recognition. These features made the iris ideal for identification purposes. It was also not easily damaged, and changes in pupil size under different conditions did not significantly affect the iris scan. It was an externally visible and highly protected organ, enabling simple scanning and reducing the risk of 'spoofing'. In addition, if removed or once a person had died, changes occurred in the eye that ensured that it would not be possible for someone to use another person's biometric fraudulently under such circumstances.
- 36 There were people who could not present an iris, for example individuals who had an opaque iris or who did not have an eye. Such problems also occurred with other biometrics, for example fingerprinting for a person with very smooth or missing fingers. To avoid these difficulties it might be preferable in some situations to use multiple biometrics.
- 37 One limitation of using iris scanning for identification purposes, as with other biometrics, was that it would be inaccurate if the details used at enrolment were incorrect or false. Nevertheless, it ensured that one person could only be associated with one identity on the system, which eliminated the possible use of multiple identities. There was some discussion about whether it was advantageous for an individual to be allowed to have multiple identities, and the point was raised that, under common law, individuals were permitted to assert multiple identities as long as there was no fraud, tax evasion or other criminal activity.

Use of biometrics for legal, forensic and police purposes

- 38 The main biometric technologies currently in use were iris scanning, fingerprinting, DNA sampling and facial recognition. Other biometrics involved footprints, odour, gait and hand veins. Different biometrics had different utilities in relation to legal, forensic and police purposes.
- 39 The latency of DNA and fingerprints meant that they were particularly useful for forensic purposes. If they were found at a crime scene, they could be matched with other records to identify and/or eliminate suspects.

As discussed earlier, DNA could also be used to reveal other information about an individual that might allow them to be traced. For example, it could be analysed to determine certain characteristics of the person, for example their sex, and in some cases hair and eye colour, and in familial searching. It was also noted that iris patterns are not genotypic (determined by the genome), and there is therefore no familial resemblance. Iris scans cannot allow people to be traced through their family.

- 40 There was some discussion over the reliability of DNA and fingerprints as biometric evidence. DNA and fingerprints of a number of individuals may be detected at a particular scene, and deliberate or accidental contamination can occur. However, it was recognised that a correct match between an individual and a crime scene did not mean that the individual had committed a crime and it was reported that the Crown Prosecution Service would not prosecute someone on the basis of DNA evidence alone. Some other evidence or proof of opportunity would be required.
- 41 At present, it seemed that most deployments of iris scanning biometric technology were for convenience rather than for police or legal purposes. Iris patterns were somewhat lacking in forensic value as they were not left behind at crime scenes. However, due to their high degree of complexity, they had a high standard of identification, which could be advantageous if they were to be used for surveillance purposes, perhaps in a similar way to the use of closed-circuit television (CCTV). The technology could not at present be used for surveillance purposes because it used arms-length scanners that required an individual to cooperate in order to be scanned. However, 'iris on the move' scanners that scanned from several feet away, perhaps without the subject's knowledge, were currently being developed. There was some discussion over whether the use of this technology for surveillance would be appropriate and proportionate to any advantages that may ensue.
- 42 The delegates also considered whether the introduction of new biometric technologies would encourage people to seek new ways to avoid detection by police and forensic teams adopting them. It was noted that criminals continued to leave DNA and fingerprints at crime scenes although it was well known that these were used for identification, and that iris patterns would be difficult to fake or conceal. A 'liveness test' that ensured that the iris being scanned was in the eye of a living person acted as a further safeguard.

Privacy and identity

- 43 Delegates considered whether biometric technologies could be considered to invade privacy or protect it. It was suggested that this would depend on the factors affecting their use. Biometric technologies could perhaps protect privacy if used to secure access to personal data or as a means to secure identification without the need to link to extensive corroborating data. However, it was suggested that such arguments were not durable.
- 44 It was important to consider positive or negative effects of biometrics for various parties, including the individual, the state and also commercial interests. Such effects could result from usage of data for unauthorised/invasive purposes or by unauthorised/invasive parties, false claims of identity and denial of services for which biometric proof of identity was required. Denial of services to which an individual was entitled, such as state benefits, for any reason relating to unwillingness or inability to contribute biometric information would be particularly undesirable.
- 45 The notion of identity was discussed, and whether this should be considered as 'what I have' or 'what I am'. By their nature, biometric technologies identified the physical self, the 'what I have', rather than the conscious self, the 'what I am'. It was commented that this could be seen as a restoration to some extent of the balance of physical and virtual body in a society in which the latter was becoming increasingly dominant.

Public awareness and perceptions of biometric technologies

- 46 Public acceptance of biometric technologies was discussed. This could depend on risks, exposure and also social convention. If such technologies were widely accepted in the future, it might be that risk and exposure became less important in public perceptions.
- 47 As part of everyday life, humans identify one other. Biometric identification technologies could be considered to be an extension of process. However, it was suggested that people's perceptions of biometric identification differed categorically, and the question was raised as to why this might be. It was suggested that people may have concerns about what information may be obtained and how it could be used, and whether it might be a target for 'hacking'. There were also fears about perceived risks of incorrect matching in such a large-scale automated process, and what the consequences might be if mistakes were made in terms of both rectifying the error and not being correctly identified. The scale and speed of the process could lead to quantitative and qualitative differences between automated identification technologies and identification by other individuals. In addition, it was suggested that

people might disapprove of the involvement of the state in this matter, and may have concerns about a 'surveillance state'.

- 48 Concern was expressed over the lack of informed public debate on these issues. It was noted that the Human Genetics Commission was planning a project on public involvement in forensic use of genetic information, which, it was hoped, would encourage public debate.

Security

- 49 Security was considered to be an important feature of biometric technologies and forensic databases, particularly as these might make attractive targets for 'hacking'. It was suggested that although the development of secure technology might initially be a priority, there could be a tendency to neglect this once the technology and organisations responsible became established. Where commercial companies were involved, there might be competition that would favour the development of systems with high standards for security and other features at the early stages, but if a monopoly were subsequently established, this might no longer be the case.

Consent

- 50 The participants discussed to what extent consent should be obtained in relation to obtaining, using and storing biometric data, and what would be permissible without consent.
- 51 In the situation of 'iris on the move' scanning, which did not require subject cooperation, it would be technically possible to take biometric information and track a person entirely without consent. It was noted that consent was not required for the use of CCTV because a person's face was in the public domain, and it was suggested that the same reasoning could apply to the iris. There was also an issue about which characteristics of an individual could be considered public if they had not specifically volunteered to share them.
- 52 The point was also raised that in some situations people who chose not to consent or participate might be denied some benefit. For example implementation at airports in the USA had meant that anyone wishing to travel there must comply with regulations on providing biometric data. In this situation consent was presumed and individuals that travelled had no choice but to comply. This regulation was justified on the basis of the benefit to national security. In other situations, refusal to participate could lead to denial of services of great importance to the individual, such as state benefits. However, the suggestion was made that anyone claiming

rights from the state could be considered to have a duty to prove their identity, and as such could be required to participate in the biometric programme.

- 53 In the use of biometrics for police and forensic purposes in which obtaining consent might not be possible or appropriate, the principle of proportionality was felt to be important ie balancing the costs, benefits and risks to individuals and the community. However, in a commercial context, proportionality in consent might not be appropriate and greater safeguards may be needed in order to protect individuals. In this context there were difficulties associated with determining proportionality when there was a commercial influence in determining the costs and benefits and the main benefits were not necessarily seen by the individuals involved.

Ethical principles and protection

- 54 The Chair invited the participants to consider what the ethical principles might be relevant to these various issues and how ethical protection could be ensured. The concept of proportionality was raised, i.e. that infringements of any rights should be proportional to the risks and benefits resulting from this infringement. Others raised concerns about whether it was appropriate to infringe human rights for the sake of utility and questioned whether the uses of bioinformation described above were compatible with the Human Rights Act. The point was made that in law it was permissible to infringe people's rights if this was done in order to protect the rights of others.

International uses of bioinformation

- 55 The current situation in France regarding biometrics and DNA databases was discussed, and a number of differences in policy and practice were highlighted. In France identity cards involving a biometric had been in use for some time, and were widely accepted. On the other hand, there were fewer security and surveillance measures, such as CCTV, in place. Regarding the collection of DNA it was reported that there were strict regulations and safeguards in place to prevent abuses, and in addition, samples from people who were not subsequently convicted of a crime were not kept.

Future prospects

- 56 Participants commented that the Workshop was a timely contribution to a broad ranging and current debate. There had been public concerns over the levels of confidence and trust in the forensic use of bioinformation

and there was a perception that there was a lack of ethical oversight. A number of delegates supported the idea of the Council exploring this issue further from an independent perspective, hoping that this would contribute to and encourage public debate and give guidance to policy-makers. It was suggested that it would be useful if this were carried out as soon as was practicable, given the current state of development of these technologies and policies regarding their use.