Chapter 7

Governance and ethical oversight

Governance and ethical oversight

Introduction

7.1 In this chapter we emphasise the importance of robust ethics and governance oversight of forensic databases, both as a means to protect the liberty, autonomy and privacy of those whose details are recorded on such databases, and also to help engender public trust and confidence in their existence and use as part of a criminal justice system. The potential uses and abuses of forensic databases are considerable. Effective governance helps to ensure not only that their utility is maximised, but also that their potentially harmful effects – such as threatening privacy, undermining social cohesion and aggravating discriminatory practices – are minimised. Good governance can anticipate and respond to new challenges; it is not merely a means to impose sanctions once things go wrong. Moreover, open governance can address suspicion and promote support among the public for an enterprise which, after all, is essentially in the public interest.

7.2 Forensic databases form an integral part of forensic science services as a whole, so discussion must also necessarily consider broader questions about forensic science in the United Kingdom, including the regulation of forensic science in general, the shift in status of the Forensic Science Service (FSS) from a public body to a Government-owned company (GovCo) and the growing private market in forensic science services. A recent Home Office consultation on the need for regulatory reform of the forensic sciences has indicated radical changes to the regulation of forensic sciences in the UK, citing a demand for greater clarity and regulation, and proposing the creation of a new Forensic Regulator.[1]

7.3 This Report has already identified some of the future regulatory challenges for forensic science services. They include the evolution of technological measures and go beyond the current possibilities of the National DNA Database (NDNAD) and IDENT1 fingerprint database, and look to a time when linkage across various types of forensic database might be possible. In governance terms, this requires considerable foresight and the need to establish frameworks that can meet new challenges as they emerge. It is important therefore, not to compartmentalise the issues, but to think more broadly and to consider how the forensic world might look in the future. Such a holistic approach is envisaged by the NDNAD Strategy Board which has reported that the role of the Forensic Regulator will extend to oversight of all forensic databases in due course.[2] Our recommendations anticipate this eventuality.

The private market in forensic science

7.4 The privatisation of the FSS, prompted by the McFarland Review in 2003,[3] has only partly been realised, although plans for a Public Private Partnership remain.[4] The FSS is now run as a profit-seeking private company, with pricing and all services governed by negotiated contracts, as well as material transfer and confidentiality agreements. The creation, and rapid growth, of a private forensics market has resurrected the need for regulation of forensic services and highlighted the challenges for governance.[5]

1. Home Office Consultation Document (2006) *Standard setting and quality regulation in forensic science*, paragraph 7.
2. National DNA Database (2007) *The National DNA Database Annual Report 2005–2006*, p7
3. Home Office (2003) *Review of the Forensic Science Service* (McFarland Report).
4. For general discussion of market forces in forensic sciences, see: Roberts P (1996) What price a free-market in forensic science services? *British Journal of Criminology* **36**: 37–60.
5. Two new requests for accreditation as DNA suppliers were received by the Custodian in 2005–06, see National DNA Database (2007) *The National DNA Database Annual Report 2005–2006*, p18.

Regulatory oversight

7.5 The Royal Commission on Criminal Justice 1993 first recommended the establishment of a Forensic Science Advisory Council to oversee the regulation of forensic science and provide independent and impartial advice on forensic science. The House of Commons Science and Technology Committee in 2005 repeated this recommendation, stating that the Council should be an independent body including representatives of all the major stakeholders, with a remit to review, or commission inspections of, the use of forensic science across the whole of the criminal justice system, and to propose improvements. While acknowledging the 'regulatory gap', the Government still does not consider that a Forensic Science Advisory Council as originally conceived would be effective, and has instead sought to introduce a more limited version to support the role of the Regulator. To assess its alternative proposals, however, it is necessary first to consider what regulation has gone before, to scrutinise what has been suggested broadly, as well as specifically in relation to the NDNAD, and to contemplate the longer term.

Governance arrangements of IDENT1

7.6 The Police Information Technology Organisation (PITO) previously oversaw the development and operation of IDENT1 – the national fingerprint database that has superseded the National Automated Fingerprint Information System (NAFIS). PITO was subsumed by the National Policing Improvement Agency (NPIA) in April 2007. The NPIA aims to align the work of different groups within policing (including those in charge of training, research and information technology) with business change within the police organisation, connecting more closely the 'front end' operations of policing with the 'back end' support and research operations.

7.7 A number of structures are in place to oversee operations and policy. The Identification Programme Board authorises and governs IDENT1 as part of NPIA's Identification Programme. IDENT1 has a Project Board, which is responsible for reporting to the Programme Board on developments and for ensuring that the project is on track and meets the requirements set out by the users. IDENT1 also has a User Board (IUB) drawn from the fingerprint expert community, and a User Liaison Team, made of up of specialists who communicate with users and identify service improvements required, maintaining regular contact with police forces and stakeholders. The Association of Chief Police Officers (ACPO) has a National Fingerprint Board (NFB) which operates within the ACPO Forensic Science portfolio. It has 20 members drawn from the scientific support and fingerprint community, Scotland, Northern Ireland, the Police Standards Unit, and the Home Office Scientific Development Branch. The NPIA will only deal with operational issues. Changes in policy will remain the preserve of ACPO and the Home Office.

7.8 The functioning of IDENT1 may raise concerns surrounding the 'linkages' with not just the Police National Computer (PNC), but other biometric and informational databases in the future. If such linkage were to be permitted (this would require changes to law and policy) then this 'inter-operability' may open up greater possibilities for wrongful or inappropriate access, for intrusive research and for misuse. The increased likelihood of identifiability might lead to greater risk of breaches of privacy, and for mistakes during inputting and transferring of data. At present, however, there is no independent official or body charged with oversight of this resource or such linkage processes.

7.9 **In our view, IDENT1, like the NDNAD, must retain public confidence in its security, especially its protection from non-authorised access and in control of its uses. This confidence depends on ongoing scrutiny and systematic audit of its uses so that the public can be sure that data held in it are not misused or misrepresented. There should be regular public reports on the use, scrutiny and auditing of this database.**

The National DNA Database

7.10 The FSS provides all operational services for the NDNAD. This contract will be reviewed in 2008 but the criteria for review have not yet been made public. Formerly, the FSS was the standard-setting body for forensic science and maintained an oversight function with respect to the NDNAD in tandem with the Custodian based in the Home Office. Since privatisation, however, the role of the Custodian has been separated from the FSS to ensure that it stays in the public sector.

7.11 The NDNAD Custodian and his staff were formerly located in the Home Office but also moved to NPIA as of 1 April 2007. The Custodian Unit is responsible for overseeing delivery of NDNAD operations and the Standards of Performance for forensic science laboratories. The Custodian is entrusted with maintaining and safeguarding the integrity of the NDNAD and developing policy. Currently, three private organisations and four police laboratories are approved to provide DNA profiles from criminal justice and/or crime scene samples to the NDNAD.[6] While the Council for the Registration of Forensic Practitioners (CRFP) accredits individual forensic practitioners, the UK Accreditation Service (UKAS) accredits laboratories in line with the two major standards: ISO/IEC 17025 and ISO 9000:2000, and the Custodian also has stringent quality criteria and checks. However, there appears to be no formal Inspectorate function to visit and assess the quality of forensic service providers on their own premises or in respect of their handling of samples and other relevant material. The Custodian told us in his reply to our Consultation that he, together with UKAS, continually monitor the performance of laboratories and ensure that any issues are dealt with expeditiously.

7.12 The NDNAD is governed by the NDNAD Strategy Board comprising representatives of the Home Office, ACPO and the Association of Police Authorities (APA). Two members of the Human Genetics Commission (HGC) have a role in providing ethical input in the decision making. The inclusion of ethical representation was prompted by critical reports from the House of Lords Select Committee on Science and Technology in 2001 and the Human Genetics Commission in 2002.[7] The Strategy Board considers that the HGC representatives also provide lay input to the Board.

7.13 The House of Lords Select Committee had expressed concerns about conflicts of interest when the FSS was acting as both user and Custodian of the NDNAD. This was addressed by the removal of the Custodian role from the FSS to the Home Office in 2005, but questions remained about transparency and accountability. The Custodian Unit has now been removed from the Home Office, following the dissolution in 2007 of the 'Forensic Science and Pathology Unit' during a re-organisation of the Home Office, and is now situated within the NPIA. The Royal Commission on Criminal Justice,[8] the House of Lords[9] and the Human Genetics Commission,[10] have all advocated the establishment of an independent oversight body to advise and monitor on the operation of the NDNAD "to put beyond doubt that individuals' data are being properly used and protected".[11] More recently, further criticism

6. Also included are some police forces that have retained 'in-house' forensic departments.
7. House of Lords Science and Technology Select Committee (2001) *Human Genetic Databases: Challenges and opportunities*; Human Genetics Commission (2002) *Inside Information: Balancing interests in the use of personal genetic data*.
8. Royal Commission on Criminal Justice (1993) (Runciman Report) Cm 2263.
9. House of Lords Science and Technology Select Committee (2001) *Human Genetic Databases: Challenges and opportunities*, paragraph 7.66.
10. Human Genetics Commission (2002) *Inside Information: Balancing interests in the use of personal genetic data*, paragraph 25.
11. House of Lords Science and Technology Select Committee (2001) *Human Genetic Databases: Challenges and Opportunities*, paragraph 7.66

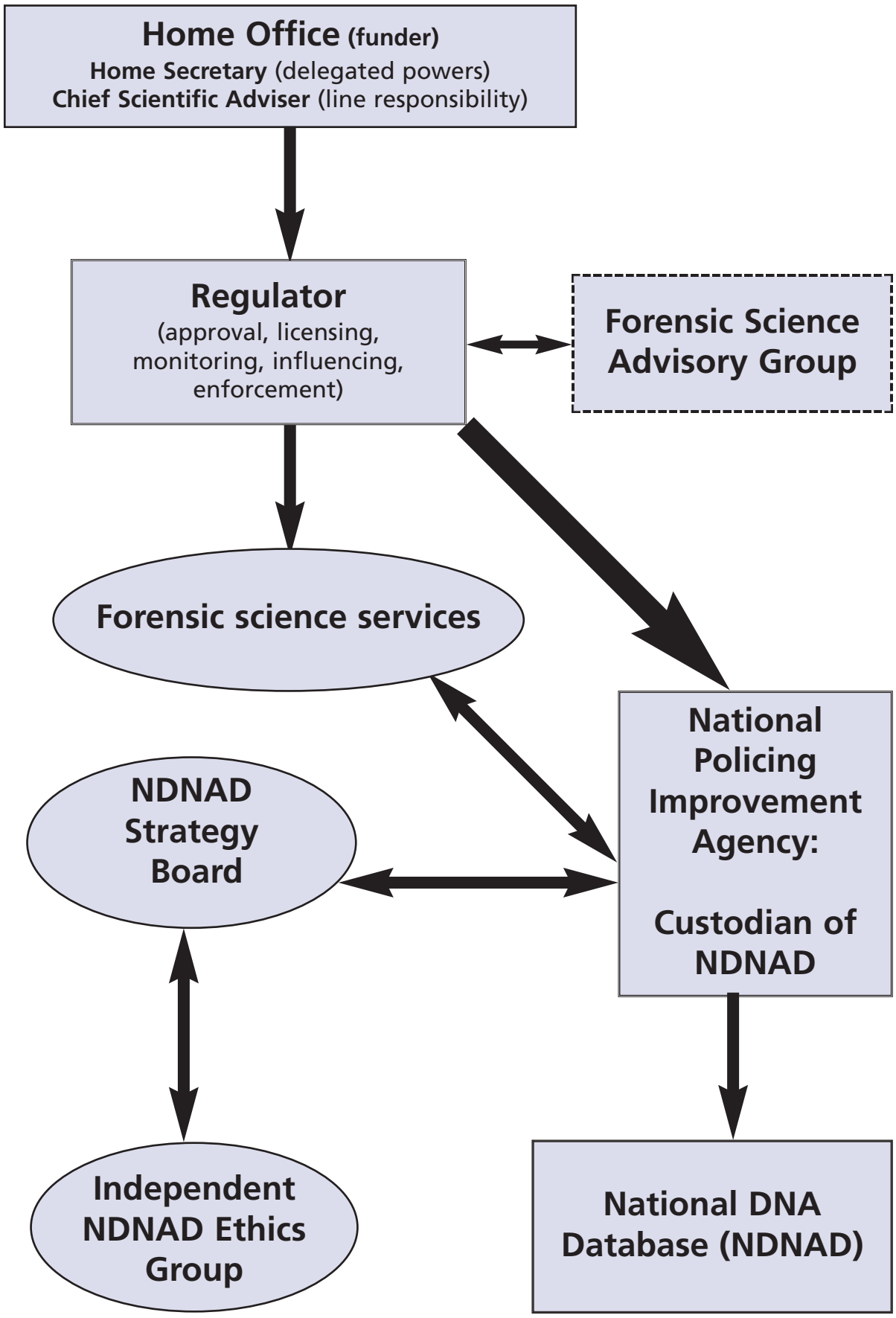
from the House of Commons Science and Technology Committee (2005) finally prompted proposals for reform.[12]

7.14 A National DNA Operations Group links the Home Office, ACPO, Scientific Support Managers within police forces, and the DNA suppliers, providing a forum for debate about the operational use of DNA. The Home Office Police Standards Unit also has a remit to ensure that DNA is used to best effect across all police forces. The NDNAD Suppliers Group supplies the DNA Board and Custodian with information relating to scientific standards and strategic developments.[13] This intricate network has meant that there has been no overarching oversight or ethical consideration of forensic services or forensic databases. The Government has stated that it is committed to appropriate ethical review and has established an Ethics Group with a specific remit over the NDNAD.[14] The challenge will be to integrate the work of this body with wider regulation of forensic services more generally.

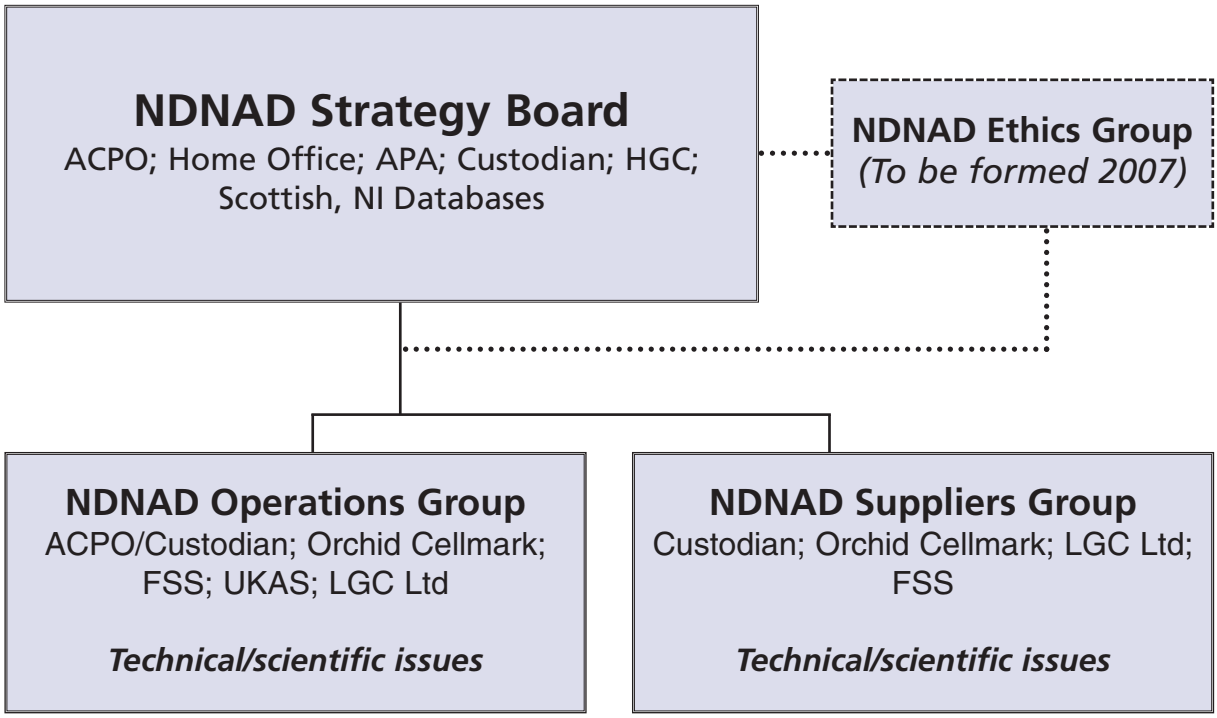
7.15 The Home Office has further proposed the appointment of a named Regulator – a Quality Adviser for Forensic Science – with personal accountability for a broad oversight remit,[15] who would receive advisory input from a Forensic Science Advisory Council (an idea re-invigorated from the Runciman Commission Report of 1993, see paragraph 7.5), which would include stakeholders in the criminal justice system, members of the scientific community and lay representation. The post would provide an overarching function for approval, monitoring, licensing and enforcement across the range of forensic services, leaving well-functioning sectors intact and intervening where gaps were found. The recommendation is that the individual would be appointed by the Home Secretary with delegated powers, located within the Home Office, report to the Chief Scientific Adviser, and be initially funded by the Home Office. It would be a specific remit of the new Quality Advisor to oversee the operation of the NDNAD.[16] Both the Quality Advisor and the Ethics Group were optimistically reported to be starting work in April 2007.[17] However, this start date has been delayed.

12. House of Lords Science and Technology Select Committee (2005) *Forensic Science on Trial*.
13. National DNA Database (2006) *The National DNA Database Annual Report 2004-2005*.
14. Mr Vernon Coaker, Parliamentary Under-Secretary of State for the Home Department, Parliamentary Statement during debate on the National DNA Database, Hansard, 15 November 2005, column 127.
15. This would include: (1) setting standards for entry to the forensic science market; (2) setting standards for forensic science activities and processes performed by the police; (3) monitoring of compliance with these standards; (4) taking action as required to address shortfalls in performance against standards; (5) oversight and control of forensic science intelligence databases; (6) ensuring that quality standards continue to be assured and improved through development of a contestable and transparent market for forensic science, enabling the entry of new suppliers, with appropriate assurance of continuity of supply; (7) creating an environment where innovation is encouraged, with 'type approval' awarded as appropriate to new techniques or products; (8) identifying, assessing and mitigating potential future risks through modification of regulatory arrangements; (9) supporting public confidence in the contribution of forensic science to the criminal justice system and the reduction of crime and its impact.
16. Response to our consultation on behalf of the Association of Police Authorities, the Association of Chief Police Officers and the Home Office.
17. *Ibid*. An advert appeared in the national press in March 2007 inviting applicants for the Chair and up to eight members of the Ethics Group for the National DNA Database (*The Sunday Times*, 11 March 2007). Membership of the Group was announced in July 2007.

7.16 We understand that the broad architecture of the proposed governance framework for forensic sciences across the industry would, therefore, look like this:



More specifically, the governance arrangement for the NDNAD looks like this:



7.17 Other reforming measures that have been reported include: (a) the revision of consent documents for volunteers who provide samples and profiles for the NDNAD; (b) clarification of the provisions to achieve full and informed consent; (c) possible revision of the strict guidelines on removal from the Database (see below) with respect to volunteers; and (d) a role for the NDNAD Ethics Group in assessing the suitability of proposed uses of the resource for research purposes.

7.18 The proposals from the Home Office have been criticised on a number of fronts, including:

- *lack of transparency* – the Regulator will be appointed by, and exercise delegated powers of, the Home Secretary and will be housed within the Home Office;
- *issues of influence and control* – the relocation of the Custodian Unit to NPIA puts the Unit more directly in the realm of policing, leaving the Home Office with arms-length, yet ongoing, policy and overall management responsibilities;
- *questions of independence* – the role of the Regulator in relation to the NDNAD would be limited in terms of assessing its impact on the detection and deterrence of crime and public attitudes towards DNA sampling and profile retention; and
- *concerns about accountability and trust* – lack of an independent relationship from the Home Office and unclear lines of accountability and the criteria on which this will be judged.[18]

7.19 The emerging structure also gives rise to a number of questions as to the respective roles and remits of the Regulator, as well as for existing and new advisory or oversight bodies. A major concern is a lack of detail on the specific tasks and powers of any oversight body or official. Although the Government has responded to specific concerns about the NDNAD and has now

18. See, for example, Liberty (2006) *Liberty's Response to the Home Office Consultation: "Standard Setting and Quality Regulation in Forensic Science"*; and GeneWatch UK (2006) Submission to the Home Office Consultation; and British Academy of Forensic Science (2006) Response to the Home Office Consultation Document.

taken steps in respect of that Database by establishing the Ethics Group, broader issues remain relatively unaddressed: for example those mentioned in Chapter 6 about the extended uses of the NDNAD, the transparency of non-operational research and the retention of information by private DNA analysis providers. At the time of writing, it is unclear what the exact remit and powers of the Ethics Group will be. The public advert for a Chair and members is silent on the issues, while the NDNAD Annual Report for 2005–2006 states that the Strategy Board will have discretion over whether or not to act on any advice offered by the Group.[19] This implies it may have relatively little influence.

7.20 Three main areas of governance require considerably more thought. These are: (1) accountability; (2) ethical oversight; and (3) quality assurance. Examples of good governance in each of these areas already operate elsewhere, and valuable lessons could be learned.

Accountability

7.21 A good model of openness and accountability can be drawn from within the criminal justice system in the form of the Independent Police Complaints Commission (IPCC). The IPCC was established by the Police Reform Act 2002. Its statutory basis lays out very clearly its independence and functions. These include: (a) the handling of complaints made about the conduct of persons serving with the police; (b) securing of public confidence in these matters; and (c) making recommendations or giving advice on possible modifications to these matters as necessary. While the IPCC is funded by the Home Office, its independence is enshrined in robust appointment provisions within the Act. Transparency is facilitated by a duty to report annually to the Secretary of State. These reports are then published.

Ethical oversight

7.22 The world of medical research provides a good example of ethical oversight. UK Biobank is the world's largest longitudinal study into gene–environment interaction. It aims to recruit 500,000 individuals aged 40 to 69, taking their blood and urine samples and base-line health measurements, and having ongoing access to participants' medical records throughout their lives and after death. Participation is voluntary and participants can withdraw at any time. The funders considered the scope and importance of the project required an Ethics and Governance Framework (EGF) which established the parameters within which the project would be conducted.

7.23 The EGF deals with consent, confidentiality, rights of withdrawal, access to the resource and commercialisation. Moreover, the EGF established the Ethics and Governance Council. The Council is an independent body set up following public advertisement and with external assessors on the appointing committee. Its task is to act as a guardian of the EGF, advise on its revision, and monitor and report publicly on UK Biobank's conformity with it. This means that the EGF is not merely a statement of good intentions, nor is it a set of purely abstract principles. It is a working document. The Council meets quarterly and has signed a Memorandum of Understanding with the UK Biobank Board of Directors. Its membership draws from a wide range of professional and lay backgrounds, and members are appointed in accordance with principles of public life.[20] The Council publishes minutes of its meetings, which are sometimes held in public. UK Biobank, for its part, is committed to transparency through publication of its Standard Operating Procedures (SOPs). To perform its task, the Council has full access to all relevant committees and documents of UK Biobank, and can request updates on the progress of the project at any time. The Council does not have the power to veto projects if they fail to

19. 11 March 2007 *The Sunday Times*; National DNA Database (2007) *The National DNA Database Annual Report 2005–2006*, p5.

20. The Seven Principles of Public Life were drawn up by the Nolan Committee and have been endorsed by Parliament. They are: Selflessness; Integrity; Objectivity; Accountability; Openness; Honesty; and Leadership.

conform to the Framework – UK Biobank itself holds the responsibility for ethical stewardship of the resource. If it fails, the Council will report that publicly – and such loss of public trust should vitiate the whole enterprise.

Quality assurance

7.24 It is unclear how far current proposals envisage a quality assurance inspectorate for existing and new service providers within the forensic sciences. There is a need for an independent and trusted body to undertake such a role, perhaps through licensing and regular inspection, and a possible model in this respect is the Human Fertilisation and Embryology Authority (HFEA), which has the primary responsibility for ensuring the highest quality of services in the fertility sector, as well as a custodian role over uses of gametes and embryos. The HFEA was established by statute, with clearly defined authority and powers, including an inspectorate role for fertility clinics and research facilities. Criminal sanctions are imposed for non-compliance with the principal provisions of the legislation, with revocation of licences providing a further sanction against breaches of licence conditions.[21]

7.25 **We recommend the development of a clear ethics and governance framework for the operation of the Ethics Group in order to establish:**

- **its relationship with the NDNAD Strategic Board;**
- **its remit – whether this be to monitor and/or advise or otherwise;**
- **its responsibilities for reporting publicly and handling complaints;**
- **its powers; and**
- **how it is to maintain its independence.**

Further consideration should be given to broader ethical oversight and governance in respect of the umbrella role of the Forensic Science Regulator and other forensic databases, such as IDENT1.

Data protection and human rights

7.26 There is no statutory basis for the operation of the NDNAD or IDENT1 or for their governance. Instead, the development of the law has been piecemeal, leaving uncertainty in places. Notwithstanding this, the NDNAD and IDENT1 are subject to the laws governing human rights and data protection. We have already noted the position in respect of human rights in Chapter 3 (paragraphs 3.29–3.34).

7.27 Both IDENT1 and the NDNAD are governed by European-wide data protection laws and are registered under the Data Protection Act 1998. The law requires that the processing of personal data must comply with eight key principles. These dictate that the data must be processed fairly and lawfully, for specified purposes, respecting subjects' rights. They must be accurate and up to date, and should not be transferred to any country that does not have adequate data protection. Certain exemptions apply when data are processed for the prevention or detection of crime and the administration of justice.[22] In particular, data subjects can be denied their right of access, and the requirement that the data be processed fairly and lawfully does not apply, permitting the police to share data with other agencies. (International transfer is discussed in paragraphs 7.42–7.53.)

7.28 The Police National Computer (PNC) has over 120,000 terminals across the country and holds over seven million records on individuals. Each record will typically include details of arrest,

21. Clinics are regulated through a licensing mechanism so that clinics may only provide services to the public when in possession of a licence, for which a clinic must meet certain criteria. If the clinic cannot meet the criteria, a licence may be withheld or revoked.
22. See Data Protection Act 1998, S. 29.

demographic details, a link to their entry on IDENT1, and whether a biological sample has been taken (and at what point in the process it is), but does not include the fingerprints or DNA profile itself. Thus access to the PNC does not automatically entail access to the bioinformation databases; it will only inform the user that the individual has records on these other databases. IDENT1 is used by all the police forces in England, Wales and Scotland. In addition to 45 fingerprint bureaux in England and Wales, British Transport Police, the Serious Organised Crime Agency (SOCA) and HM Revenue and Customs can access IDENT1. Approximately 1,200 police personnel have direct access to the fingerprint system as well as the Home Office Immigration and Nationality Directorate.

7.29 New ACPO Guidelines on the PNC incorporate a 'step-down model', which restricts access to certain data for non-police users after certain time limits. This permits the police to continue having access to data which non-police agencies should no longer be able to access. Time limits are determined by reference to the age of the subject, the final outcome of the case, the sentence imposed and the category of offence. For example, records for convictions for serious crimes receiving custodial sentences of over six months are not 'stepped down', so details remain available to non-police agencies. Information that relates to events that do not result in a conviction are 'stepped-down' when they are entered onto the PNC, making them unavailable to non-police agencies, although the details remain visible to police when using the PNC. Applications by non-police bodies to access records on the PNC are considered by a Panel chaired by the ACPO lead for Recording and Disclosure of Convictions.[23]

7.30 Access to the NDNAD is currently an arcane procedure because there appears to be no public documentation that sets out a dedicated access policy. The Custodian controls access and it is simply stated that access is restricted to a small number of people for the purposes of the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person, as laid down in the Police and Criminal Evidence Act 1984 (PACE). The NDNAD Annual Report 2005–2006 states that all requests for access to biological samples or data for research purposes are considered by the NDNAD Strategy Board. The Board takes account of a range of issues, including the legality of the purpose of the request, the requirements of the criminal justice system, data protection laws and the public interest.[24] Advice can be taken from the lay members of the Board (from the Human Genetics Commission) as well as from the Information Commissioner if necessary. It is anticipated that the newly established NDNAD Ethics Group would also have a role to play in access requests, at least those involving research.[25] It is interesting to observe that no equivalent group is envisaged for IDENT1 or other forensic databases. In addition, although it might be argued that this is because they are not concerned with such sensitive data as the NDNAD, the prospect of their future linkage to increase the overall power of their cumulative effect does give rise to concerns about increased risks to privacy. Which body or official will consider applications for linkage or research in the future?

7.31 As stated previously, the private companies storing the biological samples on behalf of police forces regularly access these samples for quality assurance procedures or for re-analysis for match verification purposes. Access to identifying information, so that the DNA provider could be identified, appears to be strictly controlled, and any proposal for access for research purposes would require permission from the Strategy Board. In addition, it has been stated in a ministerial statement to the House of Commons that any extension to the uses to which the NDNAD may be put would be subject to public scrutiny and debate.[26] Sensitivities over potential (ab)use

23. ACPO (2006) *Retention Guidelines for Nominal Records on the Police National Computer*.
24. National DNA Database (2007) *The National DNA Database Annual Report 2005–2006*, p43.
25. Response to our consultation on behalf of the Association of Police Authorities, the Association of Chief Police Officers and the Home Office.
26. Mr Vernon Coaker, Parliamentary Under-Secretary of State for the Home Department, Hansard, 15 November 2006, column 125.

suggest that, for example, searches for information on genetic relations would remain proscribed. Yet access to forensic databases for research purposes remains an under-regulated area, and may remain so while the criteria themselves remain vague (see Chapter 6).

7.32 **In addition to the recommendations made in Chapter 6, we recommend not only that there must be robust procedures for assessing applications for research access to the NDNAD and stored samples, but that there should also be a requirement to articulate publicly the basis upon which applications for any access to data stored on bioinformation databases will be considered and the precise purposes for which access will, and will not, be granted either to police or non-police agencies.**

The importance of independence

The discretion of Chief Constables to remove profiles and samples

7.33 Public trust and confidence will not be maintained if arrangements and procedures are perceived to be partisan or self-serving. A good example of a problem area in this regard is the current provisions for handling requests to remove profiles from the NDNAD or to destroy samples or fingerprints. Individuals are able to request the removal of their individual record(s) from the PNC and linked databases such as IDENT1 and the NDNAD. There is uniform guidance provided by ACPO to Chief Constables regarding the removal of such records. This guidance states that records should only be removed in 'exceptional cases', which may include those where the arrest or sampling was unlawful, or where there was no offence prompting the arrest. The applicants themselves must demonstrate why their case is exceptional.[27]

7.34 Once these guidelines become established, a library of precedents will be maintained on what has previously been considered 'exceptional'. Yet although the guidelines are intended to ensure consistency, there is no substantive guidance on how to determine if a case is exceptional. Decisions therefore risk being arbitrary and potentially unjust. It is not clear, for example, if misconduct or police error could be grounds for removal, such as in the case of mistaken identity and arrest involving a juvenile who could not then have his profile erased despite the error.[28] There is no apparent appeal process, although it is assumed that a judicial review of a decision by a Chief Officer would be possible.

7.35 This approach is to be contrasted with the position in Germany where authorities must show a likelihood that someone will (re)offend with a recordable offence before retention of samples is possible (see Box. 4.3). Thus, in Germany and indeed Scotland, the state must justify retention, whereas in England and Wales the burden falls on the individual to show why retention should not be permanent (see Chapter 4).

7.36 We have earlier recommended that while indefinite retention of fingerprints and DNA profiles is justified from those convicted of a recordable offence (paragraph 4.54), subject samples and the resulting profiles of those not charged or convicted should be destroyed except in the case of serious violent and sexual offenders – where Chief Constables may apply to a court for retention for two years (paragraph 4.55). We have also suggested a presumption in favour of the removal of records of minors.

27. *Exceptional Case Procedures for Removal DNA, Fingerprints and PNC Records*, April 2006, available at: www.acpo.police.uk/policies.asp, accessed on: 11 July 2007. See also, *ACPO Retention Guidelines for Nominal Records on the Police National Computer*, Appendix 2, 2006: www.homeoffice.gov.uk/documents/Bichard_Step_Model_Retention.pdf?view=Binary, accessed on: 11 July 2007.

28. Taylor N and Roberts A (2006) Genes on record: one size fits all? *New Law Journal* **156:** 1354; 9 January 2006 *Daily Telegraph*.

7.37 **At present, the 'exceptional circumstances' criteria for removal of records from the NDNAD and other databases are too restrictive, and the Chief Constable's discretion too wide. If the current system remains and records are not automatically removed for those not convicted, in accordance with our earlier recommendations (paragraphs 4.53–4.55 and 4.72), we recommend that:**

- **There should be public guidelines explaining how to apply to have records removed from police databases, and the grounds on which removal can be required.**
- **The police should be required to justify the need for retention in response to a request for removal of an individual (with a strong presumption in favour of removal in the case of minors, see paragraph 4.72).**
- **An independent body, along the lines of an administrative tribunal, should oversee requests from individuals to have their profiles removed from bioinformation databases. The tribunal would have to balance the rights of the individual against such factors as the seriousness of the offence, previous arrests, the outcome of the arrest, the likelihood of this individual re-offending, the danger to the public and any other special circumstances.**

The integration of forensic databases: the emerging challenge of linkage

7.38 Moves to integrate forensic bioinformation databases with each other and with other police and criminal records databases have recently become a priority.[29] However, any integration must retain the integrity of the individual databases, and ensure that safeguards are in place to protect the data from misuse. The possible 'sharing' or cross-referencing of forensic databases, as well as the potential for forensic use of non-forensic databases or the non-forensic use of forensic databases, are a possible further cause for concern. Many of our respondents and those who gave oral evidence pointed to the risks associated both with increased linkage and the cross-over between civil 'security' and criminal justice databases. There are also fears that as databases containing sensitive personal data proliferate (including databases for medical research such as UK Biobank and even databases for the fingerprints of schoolchildren, see paragraph 4.6), police access under some circumstances may be harder to resist in the future.[30]

7.39 The House of Commons Science and Technology Committee has pointed to the potential of linkage to other (forensic) databases and recommended that the police and the Home Office pay adequate attention to custodian and access arrangements as well as data sharing mechanisms.[31] We have offered the example of IDENT1 as a platform that currently exists and which is ideally suited to facilitate record linkage across an entire range of forensic databases in the future.

7.40 While the variety of forensic biometric databases are not currently linked in any sophisticated fashion, it is a stated aim for databases to be 'inter-operable' in the near future.[32] The ethical implications of such databases could then be 'multiplied' by linking with other databases, most particularly with respect to concerns about privacy. Those concerns may be further compounded if linkage is envisaged between databases across different countries, as we discuss in the next section.

29. See, for example, the Bichard Inquiry into the Soham murders, whose recommendations included a national information technology system, adequate investment in the Police National Computer and a new code of practice on information management, see http://www.bichardinquiry.org.uk, accessed on: 16 July 2007.
30. Note, however, both UK Biobank and its sister project, Generation Scotland, have indicated that they would vigorously resist any attempt by police for access to their genetic resources.
31. House of Commons Science and Technology Select Committee (2005) *Forensic Science on Trial*, paragraphs 90–9.
32. See (most recently) *PITO Business Plan 2006/07*.

The challenges of international exchange

7.41 Countries throughout the European Union and beyond are expanding their bioinformation databases,[33] and demands are increasingly being made for data to be shared among international law enforcement agencies. The importance of cooperation over DNA technologies in particular is recognised by domestic and international law enforcement agencies.[34] The European Commission has expressed a desire that there be direct, online access to DNA databases across Europe.[35] However, current barriers to safe and efficient sharing include:

- disparate legal regimes on the protection of DNA and genetic data, albeit that the Data Protection Directive is a Europe-wide instrument;
- disparate collection regimes for the taking and retention of DNA: the United Kingdom has by far the most permissive regime in Europe with a DNA database larger than the sum of all others in the Union;
- absence of legal agreements on sharing and exchange of data (see. Prüm Treaty, paragraph 7.50);
- non-standardisation of databases and formats across countries;
- lack of compatible technical systems to ease sharing and ensure inter-operability;
- need for all countries to meet minimum agreed standards on information held on databases; and
- paucity of formal procedures to facilitate cross-border investigation and data sharing.

7.42 **We recommend, on the basis of standard European data protection principles, a minimum set of safeguarding requirements to consider before allowing access to bioinformation databases to international law enforcement agencies, which would be:**

- **to ensure there is a sufficient level of data protection in all authorities/agencies that would receive information;**
- **to subject each request to adequate scrutiny as to merit and reasonableness and on a transparent basis;**
- **to agree the criteria for sharing data, for example only for the investigation of serious crimes or in special circumstances; and**
- **to share only as much information as is necessary to meet the request and only to those authorities or agencies which 'need to know'.**

7.43 European Technical Standards fall within the auspices of the European Network of Forensic Science Institutes (ENFSI), which has agreed processes to facilitate exchange of forensic data. The ENFSI DNA Working Group has agreed a standard common seven markers as a minimum DNA profile. In practice, most countries, including the United Kingdom, rely on standards that require more markers (SGM+ uses ten markers). This could raise issues about variation across Europe and could increase the error rate. A common safeguard, however, is that a match alone cannot lead to prosecution in the absence of further evidence (see Chapter 5).

7.44 Exchanges of data are currently made on a case-by-case basis, with no internationally agreed

33. See European Network of Forensic Science Institutes DNA Working Group (2006) *Report on ENFSI Member Countries' DNA Database Legislation Survey*.
34. Parliamentary Office of Science and Technology (2006) PostNote *The National DNA Database*, Number 258, p3.
35. As an alternative to direct access, requests for data can be handled internally by a governance body and the enquirer can be provided with data that are suitably protected, e.g. through anonymisation. Such a model operates within the UK health services for certain kinds of health research. Such requests are scrutinised by independent dedicated bodies, namely the Patient Information Advisory Group in England and Wales and the Privacy Advisory Committee in Scotland.

framework for sharing data.[36] Various initiatives are underway to facilitate exchanges while maintaining quality standards and adequate levels of protection for individual rights. This is important because, as noted in paragraph 7.27, not all countries have the same safeguards in place for the protection of data. Because the integrity of forensic databases is vital to ensuring public trust and confidence, greater sharing of sensitive personal data across national borders may be problematic. The process of exchanging DNA profiles entails 'personal' information leaving the jurisdiction in which it was obtained, with little by way of assurance that it will not be subjected to unauthorised storage and use. There is no oversight body to monitor the international exchange of DNA profiles, nor any organisation that could make enquiries (and pursue complaints) on behalf of individuals whose data have been misused. Concerns over such a lack of oversight are heightened by recent proposals for a centralised database of fingerprints across the European Union, with an attendant obligation on each Member State to transfer details held by national police forces to a central authority.[37]

7.45 Interpol established a DNA database in June 2003, for the use of member countries to compare selected DNA profiles they have collected with those collected by other member countries. This database became operational at the end of 2005. It is directly accessible for single or multiple requests by 33 member countries who may contribute to the database. Interpol has protocols for international exchange of data on a case-by-case basis, with DNA profiles able to be stored and searched across international borders using the Interpol Standard Set Of Loci (ISSOL). There have been two significant exchanges of DNA information in the past three years, with the United Kingdom sending unsolved crime scene profiles overseas in an effort to produce a match with a subject profile held on a DNA database in another country. In October 2004, 1,687 DNA crime scene profiles from undetected sexual offences in the UK were submitted to the Interpol DNA database (through the UK National Central Bureau for Interpol (NCB)). In February 2006, 10,763 DNA crime scene profiles from unsolved serious crimes committed in the UK were sent to the Netherlands for checking against the Netherlands DNA database.[38]

7.46 An Interpol DNA Charter has been developed to provide a suitable regulatory framework. Oversight is provided by a DNA Monitoring Expert Group (MEG) which comprises leading DNA experts from member countries. There is a proposal to allow individual countries to retain DNA within their borders but to allow searches by other countries (the UK's preferred option). The UK NCB undertakes risk assessments of all requests for searches to be undertaken against the NDNAD from overseas law enforcement agencies. It is not known on what basis this is done, although searching has been carried out through the NDNAD Custodian. The number of overseas requests that have been granted to exchange DNA information from the UK is small: 121 subject profiles from the NDNAD were provided to the UK NCB between August 2004 and May 2006, while 398 NDNAD search results (from running unsolved crime scene samples from overseas against the UK NDNAD to see if any subject profiles produced a match) were provided to the UK NCB in response to overseas requests in the years 2004/5 and 2005/6.[39] Interpol has recently launched a DNA Gateway, to which the UK is a signatory, and by which DNA profiles can be compared online for matches. Profiles are held anonymously.[40] The Interpol database is not used for familial searching.

7.47 Whilst DNA profiles are sent outside the United Kingdom under exemptions in the Data Protection Act 1998, there has been no systematic Government consideration of this specific

36. Since 2004 there have been 519 requests from foreign countries from information from the NDNAD; Joan Ryan MP, 5 June 2006, Hansard, column 278W.
37. Charter D (2007) Central fingerprint database plan draws fire from all over EU *The Times*, 16 March.
38. Andy Burnham MP, Hansard, 18 April 2006, column 446W.
39. Joint response to our consultation on behalf of the Association of Police Authorities, the Association of Chief Police Officers and the Home Office.
40. National DNA Database (2007) *The National DNA Database Annual Report 2005–2006*, p45.

issue. Nor are there guidelines for the handling and exchange of DNA profiles other than those set out in the general provisions of Title VI of the Treaty on European Union (which provides for a 'bridge' between member countries to achieve the objectives of the Union, and sets out 'common interests' such as justice and home affairs, which members agree to cooperate upon), and in Title IV of the Europol Convention (which outlines parameters for the storage and use of personal information).

7.48 The European Union's ambitions for strengthening freedom, security and justice include an aspiration for borderless flows of information from 1 January 2008. The European Council Framework Decision of 2005 has sought to promote this objective while ensuring the protection of personal data exchanged between police and judicial bodies of Member States.[41] Conditions to be observed include: protecting sources, maintaining confidentiality, achieving common standards for access as well as common technical standards for sampling and profiling, and uniform protection of individuals from abuse. This Framework Decision would require that personal data used by competent authorities must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive;
- accurate and, where necessary, kept up to date; and
- kept in a form that permits identification of data subjects for no longer than is necessary.

7.49 The Framework Decision concerns information exchange of six kinds of data, including DNA and fingerprints, and introduces direct (online) access to databases. Europol would have same rights of access. The primary obligation is to forward information directly to a requesting party, save in certain specified circumstances, for example, to protect individuals, or to protect confidentiality or other fundamental freedoms.

7.50 The Prüm Treaty (2005) is an existing cooperation agreement of eleven Member States[42] for exchange of information and has been offered as a model for the entire European Union. It provides for:

- direct access to foreign databases on a hit/no hit basis;
- automated comparison of profiles of untraceable people by mutual consent (again on a hit/no hit basis); and
- collection of biological samples and supply of DNA profiles.

7.51 The direct access provisions would not apply until the data protection elements of the Treaty have been adopted into national laws. The Prüm Working Party has also recommended that new laws would be required in signatory countries to allow familial searching under the Treaty. Importantly, the 2007 German Presidency proposed that the Treaty be transposed into EU law, which would then require it to be implemented into the laws of all 27 Member States. Any such initiative would, however, require unanimity to be adopted, and this may take several years with no guarantee of success.

7.52 These initiatives were recently considered by the House of Lords European Union Committee which expressed considerable disquiet about the way in which a multilateral treaty like Prüm had made its way onto the EU legislative agenda.[43] Although there are constitutional and

41. Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *Official Journal* L 069,16/03/2005 P. 0067–0071, available at: http://ec.europa.eu/justice_home/doc_centre/privacy/law/index_en.htm, accessed on: 6 July 2007. Member States had to take necessary measures to comply with the Decision by 16 March 2007.
42. Austria, Belgium, France, Germany, Luxembourg, the Netherlands, Spain, Finland, Italy, Portugal and Slovenia.
43. House of Lords, European Union Committee (2007) *Prüm: An Effective Weapon Against Terrorism and Crime?* HL Paper 90.

procedural issues at stake, these are not the concern of this Report. Rather, the value of the House of Lords report lies in its identification of key matters which must be addressed before there is any progress towards European harmonisation, whether this be by means of the Commission's Decision Framework[44] or a modified version of the Prüm Treaty.[45] Two recommendations of the EU Committee are directly pertinent to our conclusions and we endorse them here as recommendations. **The threshold for holding DNA profiles on a forensic database is far lower in the United Kingdom than in any other Member State of the EU, and the proportion of the population included on the UK DNA Database is correspondingly far higher than in other EU countries. The Government should as a matter of urgency examine the implications of DNA exchanges for those on the United Kingdom NDNAD. The Government should insist on the inclusion in the Prüm Treaty of provisions to ensure that its operation is properly monitored. At the very least, the following is required:**

- **an obligation on national agencies to produce annual reports, including statistics, on the use of their powers under the Treaty; and**
- **an obligation on the European Commission to produce an overall evaluation of the operation of the Treaty, for submission to the European Council, the European Parliament and national parliaments, to see whether it needs amendment.[46]**

Despite a Europe-wide data protection regime which has existed since the adoption of the Data Protection Directive in 1995, specific matters as they relate to 'police and judicial cooperation in criminal matters' – the so-called 'third pillar' of the EU – have not been addressed in any depth. The Government should seize the opportunity to stipulate that they will agree to the Prüm Treaty only if other Member States simultaneously agree to a Framework Decision setting high standards for the protection of data across the third pillar.[47]

7.53 In summary, privacy-related issues concerning the use and transfer of DNA and other data for inter-jurisdictional criminal matters must be considered and agreed *in parallel* with arrangements for availability, exchange and linkage.

The future in the United Kingdom

7.54 The current regulatory structure is not on a statutory footing and the legislative framework surrounding the forensic use of bioinformation is piecemeal and patchy. The regulatory architecture of forensic services is also currently in a state of flux in the United Kingdom. While different areas of the industry might require specific attention, such as the NDNAD, there is a need to think more holistically and prospectively about the future possibilities and challenges that might come with increased access to, and sharing of data, across forensic databases. An essential aspect of all governance arrangements must be a commitment to transparency and openness both as regards standard operating procedures (SOPs) and decision-making processes. This is in addition to the requirement that those procedures and processes be justifiable in the first place. Another crucial feature of the regulatory structure is the role of an independent oversight body or official.

44. The House of Lords Committee opines that the Commission proposal risks becoming redundant, there being no further negotiations at the time of writing, see paragraph 18.
45. The House of Lords Committee urges the UK Government to take advantage of the need for unanimity to adopt Prüm at the European level in order to negotiate a better set of provisions than are currently available, Chapter 4 *What Should the United Kingdom Be Doing?*
46. *Ibid*., paragraph 80.
47. *Ibid*., paragraph 91. The European Union takes decisions in three separate 'domains' (policy areas), also known as the 'three pillars' of the EU. The first pillar is the 'Community domain', covering most of the common policies, where decisions are taken by the 'Community method' – involving the Commission, Parliament and the Council. The second pillar is the common foreign and security policy, where decisions are taken by the Council alone. The third pillar is 'police and judicial cooperation in criminal matters', where again the Council alone takes the decisions.

7.55 **We recommend that there should be a statutory basis for the regulation of forensic databases and retained biological samples. A regulatory framework should be established with a clear statement of purpose and specific powers of oversight delegated to an appropriate independent body or official. This should include oversight of research and other access requests, for example for further testing of samples or familial searching and inferring ethnicity. We are pleased to see the establishment of an Ethics Group by the Home Office, with a remit to oversee the running and uses of the NDNAD, but its specific functions and powers must be more clearly, and publicly, articulated. Moreover, we consider that a longer-term view is required that considers the future possibilities and challenges that may come with increased access and linkage involving a range of forensic databases.**

7.56 Throughout this Report we have drawn attention to the difficulty in assessing the impact of increasing police powers because of the poor quality or absence of official statistics (or conflicting statistics). Moreover, on many vital issues such as requests to conduct research on databases and/or samples or general access provisions to the NDNAD, there is an absence of protocols or guidance open to public scrutiny.

7.57 **We recommend a far greater commitment to openness and transparency and a greater availability of documents to public scrutiny. Where public access is denied for reasons of security and the administration of justice, this should be fully explained and justified. Efforts to improve the generation of data and statistics are welcomed, as are apparent efforts to increase the publication of data. These moves are still in their early stages, and their continuation is strongly supported.**