



THE FUTURE OF FORENSIC BIOINFORMATION

Carole McCartney
Robin Williams & Tim Wilson

MAY 2010



The Nuffield Foundation is a charitable trust with the aim of advancing social well-being. It funds research and innovation, predominantly in social policy and education. It has funded this project, but the views expressed are those of the authors and not necessarily those of the Foundation. More information is available at www.nuffieldfoundation.org

The Authors

Dr Carole McCartney: Senior lecturer in law at the University of Leeds. Carole has written on Australian justice, Innocence Projects, and DNA and criminal justice, authoring *Forensic Identification and Criminal Justice: Forensic Science, Justice and Risk* (2006). She established an Innocence Project at the University of Leeds in 2005, and was project manager for the Nuffield Council on Bioethics report '*The Forensic Uses of Bio-information: Ethical Issues*' (2007). She is currently an EU Marie Curie Fellow (2009-2012), working on a project entitled: 'Forensic Identification Frontiers', which sees her based at the Centre for Forensic Excellence at Bond University, Australia until September 2011.

Professor Robin Williams: Emeritus Professor of Sociology, University of Durham and Professor of Forensic Science Studies at the University of Northumbria. He has been researching the police uses of forensic science since 2000, beginning with a study of crime scene examiners in one police area, extending this to Home Office supported work on crime scene examination in several police forces, and then carrying out two Wellcome Trust funded studies of forensic DNA databasing in the UK and across the EU. He was a member of the Nuffield Council on Bioethics working party on '*The Forensic Uses of Bioinformation: Ethical Issues*' (2007).

Professor Tim Wilson: Visiting Fellow at PEALS (Policy, Ethics and Life Sciences), Newcastle University and, after the commencement of this project, Professor of Forensic Science and Public Policy at the Northumbria University Centre for Forensic Science. As a former Senior Civil Servant he has extensive experience of policy making on forensic science, the restructuring of forensic provision and regulation (including as a member of the NDNAD Strategy Board). While at the Home Office he initiated work that culminated in the 2004 announcement that the DNA Expansion Programme would be replaced with a broader and more integrated policy. He has also worked on international EU (AEGIS) and G8 co-operation projects for both the Home Office and ACPO.

Acknowledgements: The authors would like to thank all seminar attendees for giving so generously of their time and expertise throughout this project. We would also like to thank our respective institutions, Benedict Wilson for drawing figures 4.2, 4.3 and 6.1, and the Nuffield Foundation for their unstinting support.

The Future of Forensic Bioinformation

Contents

	Page
1 Introduction	1
○ Forensic Bioinformation: Locating the Issues	
○ Method	
○ Report Themes	
2 The Current Context	14
○ The Legal Context	
○ Crime and Arrest Rates	
○ Fingerprints and IDENT1	
○ DNA and the NDNAD	
○ Cost	
○ The International Context	
3 Evidence and Assessment	21
○ Evidence and Assessment	
○ Forensic Bioinformation: Existing Data Sources	
▪ Fingerprints	
▪ DNA profiles	
○ Police Force Returns	
○ Forensic Bioinformation: Bespoke Research Studies	
○ Cost-effectiveness and Forensic Science Utility	
○ Conclusion	
4 Internationalisation and Exchange	39
○ Introduction	
○ ‘Dissolving boundaries’ and ‘Securing the UK Border’	
○ International cooperation	
○ Bioinformation held outside the criminal justice system	

- The significance of Scotland
 - The legal position in Scotland
 - Data sharing between jurisdictions
 - The interplay of policy & technological developments
- Validity, technological development and DNA sample retention
 - False or adventitious matches, false eliminations and sample retention
 - Ensuring the validity of dactyloscopic information
 - The foreseeable technological obsolescence of SGM+
- Conclusion

5 Governance & Accountability 73

- The current network of forensic bioinformation governance
 - Issues and Prospects
- Scientific and Organisational Integrity
 - Quality Standards
 - Data Protection and Security
 - Scientific Research and Technological Development
 - Public Confidence and Trust
- Criminal Justice Integration
- Conclusion

6 Summary and a Proposal 109

- *Beyond S & Harper*
- Evidence and Assessment
- Internationalisation & Exchange
- Governance and Accountability
- A Proposal

1 Introduction

Forensic Bioinformation: Locating the Issues

- 1.2. The collection and use of bioinformation in support of criminal investigations and counter-terrorism measures is an important feature of contemporary efforts to ensure public safety and maintain national security. The two most important forms of forensic bioinformation - DNA profiles and fingerprints - were both initiated by British scientists and police officers, and the UK commitment to the collection and use of these kinds of forensic bioinformation has been unrivalled internationally. The National DNA Database (NDNAD) is widely acknowledged to be a world-leading innovation in the development of the forensic application of genetic technology and information management. The IDENT1 platform, hosting the national fingerprint and palm print databases, also continues to grow in size and technical capability. The scale of investment in forensic bioinformation collection and the technical infrastructures that support its investigatory and prosecutorial functions continues to be significant, reflecting public confidence and political belief in its contribution to crime detection, the administration of justice, and the risk management of known offenders.¹
- 1.3. Previous studies have examined the ways in which scientific, legislative and budgetary innovations have been brought together to materialise the rising aspirations of a number of key criminal justice and forensic science stakeholders.² There have been extensive ethical and political reflections of these developments in the UK and elsewhere. Academic research has both supplemented, and been informed by, the work of relevant Parliamentary Committees, Advisory Bodies and other civil society organisations.³ More recently, the deliberative landscape over which various forensic bioinformation claims have been advanced and defended has been irrevocably altered by the decision of the European Court of Human Rights on the legality of the current legislative framework for the collection and management of forensic bioinformation in England & Wales.⁴

¹ By early 2006 there had been investment of £150 million in IDENT1 and £300 million in the DNA Expansion Programme: Home Office, *DNA Expansion Programme 2000-2005: Reporting Achievement* (London: Home Office, 2007) pp 19 and 4.

² See for example: McCartney, C. (2006) *Forensic Identification and Criminal Justice*, Cullompton: Willan; Williams, R., and Johnson, P. (2008) *Genetic Policing*, Cullompton: Lynch, M., Cole, S., McNally, R. and Jordan, K. (2008) *Truth Machine: The Contentious History of DNA Fingerprinting*. Chicago: Chicago University Press; Cole, S. A. (2001) *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge Mass: Harvard University Press.

³ See, for example (*inter alia*): House of Commons. (2005) *Forensic Science on Trial*. Committee on Science and Technology. London: HMSO; Human Genetics Commission (2001) *Whose Hands on Your Genes?* London: Department of Health; Nuffield Council on Bioethics (2007) *The Forensic Use of Bioinformation: Ethical Issues* Cambridge; Human Genetics Commission (2009) *Nothing to Hide, Nothing to Fear* London, Department of Health; Home Affairs Committee (2010) 'The National DNA Database'; London, House of Commons.

⁴ *S & Marper v. The United Kingdom* (App.no. 30562/04) [2008] ECHR 1581 (4 December 2008).

- 1.4. Rapidly evolving technology and legal reforms continue to stimulate debate about the efficacy and ethics of the role of forensic bioinformation within the criminal justice system in England & Wales and elsewhere. The collection, retention and use of biological materials, usually without the consent of those from whom they were taken or retrieved, raises a range of policy questions. These include the scope of powers necessary for the effective and ethical collection and use of such materials, and how a balance may be achieved between the exercise of these powers by the police and the rights of individuals. However, almost all who urge caution, and many of those who promote, the future development of these technologies now seem to agree that there is a paucity of independent and authoritative research on how, and the extent to which, the information derived from them directly impacts on criminal investigations or usefully supplements other forms of information held by the police and other relevant agencies.⁵ There remains a lack of robust evidence and critical assessment of the benefits and costs of rapidly increasing expenditure in this area. It is widely argued that this shortcoming prevents informed decision-making and makes problematic the necessary efforts to justify particular levels of investment in forensic bioinformation within the legal system domestically and trans-nationally,⁶ albeit this is a systematic feature of all police resource allocation.⁷
- 1.5. The relevance of much domestic discussion on issues surrounding forensic bioinformation has been overtaken by the judgment of the European Court Of Human Rights in the case of 'S' and Marper versus the UK which was delivered in December 2008. In 2001, two individuals, 'S', an eleven year old, and Mr Marper, were arrested in separate incidents, and had their DNA samples and fingerprints taken. Neither were subsequently convicted of any offence and duly applied to their local Chief Constable to have their DNA samples and profiles destroyed. This request was denied and an application for judicial review of the denial was refused. In 2002 the Court of Appeal upheld this decision, and the case proceeded to the House of Lords in 2004. The Lords considered whether the continued retention of the DNA of 'S' and Mr. Marper, who remained unconvicted of an offence, was a breach of their Article 8 right to privacy and their Article 14 right against discrimination. The Lords decided that their privacy may have been breached (one Lord concluded that it was, the others remained doubtful), but even if it was, it was a 'modest' breach outweighed by the wider benefits to society of retaining DNA and fingerprints. The purpose of retention – to prevent and detect crime – was provided for by Article 8, and as such, the retention was ruled lawful.

⁵ The Magee Report defines information on criminality as: 'any information which is, or may be, relevant to the prevention, investigation, prosecution, or penalising of crime.' Sir Ian Magee, *The Review of Criminality Information* (The Magee Report) (July 2008) Home Office, London. p.4.

⁶ "A complex network of organisations is involved in the protection of the public... An effective public protection network demands that all work together, nationally and internationally, to improve public protection. The public expects them to do so efficiently, cost-effectively and with proper regard to their rights." *ibid.*, p.3.

⁷ Public Bill Committee, 26 January 2010, Q 79 at www.publications.parliament.uk accessed 24 March 2010

- 1.6. The European judges in *'S' & Marper v UK* took a diametrically opposed view to the House of Lords. Their unanimous decision held that Article 8 rights to privacy were indeed breached, and concluded that:

“...the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences..., fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.”⁸

- 1.7. The *Marper* judgment is significant for its decisive contribution to normative debates about the use and governance of forensic bioinformation. UK instances of these debates had been taking place, but had not directly influenced Government policy. Also, with a few notable exceptions, the questions central to the European judgment had failed to obtain more than superficial consideration from English judges. These have been reliant upon a pragmatic refuge in ‘a balance of judgment’, weighted in the Government’s favour by a failure to examine with any rigour the claims of Treasury Counsel. It is salutary to recall a similar string of ECtHR reverses relating to the ‘relaxed, some might say complacent attitude to proactive policing methods in the English courts and how this came to be resolved through the Regulation of Investigatory Powers Act 2000 (RIPA).⁹
- 1.8. Mixed UK reactions to *Marper* may reflect a particular cultural and economic context that influences attitudes towards the forensic use of bioinformation. For over one hundred years, English scientists and officials have initiated many key developments in this field, providing a model for applying modern technologies of biometric identification in a systematic and commoditised manner. Jeffreys’ discovery in 1984 of what he termed ‘genetic fingerprinting’, resulted in the use of DNA in immigration and paternity disputes, then in a murder investigation in 1986. A century on from Henry’s introduction of fingerprints, this new technology of identification was never a public sector monopoly. Indeed, private DNA analysis companies in the UK have been instrumental in the expansion of the forensic use of bioinformation. Even if profit-oriented, the pluralistic nature of this development served the cause of human rights. For example, since its creation, Cellmark Diagnostics has helped to reunite families by providing evidence of family biological relationships to successfully challenge government immigration decisions.¹⁰

⁸ *S & Marper v. UK* [2008] para.125.

⁹ Roberts, P. (2007) ‘Law and Criminal Investigation’, in Newburn, T., Williamson, T. and Wright, A. (eds.) *Handbook of Criminal Investigation* (Cullompton, Willan) p.99.

¹⁰ This is not necessarily always the case. A private sector monopoly or even technically competitive market that is wholly dependent for income on government, is unlikely to have an equally benign effect by empowering

- 1.9. These more recent technological developments occurred simultaneously with the emergence of a competitive forensic marketplace. Within England and Wales the use of DNA as an investigative technique was not held back by the problems in traditional public sector forensic science laboratories, which are ‘almost universally characterised by backlogs’.¹¹ This may influence the content of the criminal law. Most countries are likely to maintain symmetry between what can be described as the legislative and technical domains: unless government forensic laboratories have the resources, appetite for or ability to deliver additional DNA analytical capacity there is little point in passing legislation to permit the extensive forensic use of DNA.¹² Indeed, the introduction of national arrangements for the use of DNA for forensic purposes frequently precedes laws regulating such activity. Such use almost universally precedes specific database legislation. Although within the European Union there is now a pattern of enacting database legislation before the database itself is created, there are still at least six countries that may have databases but no database legislation, not even in the more limited form.
- 1.10. This aspect of UK bioinformation development, with the exception of reference to ‘privatisation’ or ‘commercialisation’ *per se*, is ignored in virtually all of the sociological, ethical and jurisprudential discourse on the use of bioinformation. It has two consequences for critics of the UK position pre-*Marper*. Firstly, it can result in inaccurate or incomplete comparisons between various countries. England and Scotland are an important example. Secondly and more significantly, it could mean that the margin of justification is a much more fragile basis for ethical and political analysis than it seems at first sight. A comparative survey of the law in different states may reflect different stages of technological development and investment rather than jurisprudential philosophy or principled political decision making. The extent to which the use of DNA and the creation of databases precede legislation suggests that conclusions drawn from comparisons of statute books have to be treated with caution. On the street and in the laboratory, criminal justice may operate differently.
- 1.11. For the advocates of a more maximalist approach to DNA profiling and retention, such as represented in the UK Government’s response to the *Marper* judgment (*‘Keeping the Right People on The DNA Database: Science and Public Protection’*) the consequences are equally significant. First, in a commercial forensic market, how can some of the key parties, whose voices are critical and dominant because of their privileged access to expertise and information, demonstrate that whatever they advocate is not influenced by commercial interests or professional ambitions?

individuals to defend their human rights against an oppressive state or its agents such as the police, on, the other hand, a state forensic laboratory monopoly would equally leave citizens disadvantaged. Ultimately, this requires an effective separation of powers within the executive, legislative, judicial and regulatory structures of the state.

¹¹ Fraser, J. (2006) ‘The application of forensic science to criminal investigation’ in (eds.) Newburn, T., Williamson, T. and Wright, A. *Handbook of Criminal Investigation* (Cullompton: Willan)

¹² Wilson, T.J, Forensic science and the internationalisation of policing’ in Fraser, J. G. and Williams, R. (Eds) *Handbook of Forensic Science* (Willan Publishing), 2009, pp.509-512 and Figure 18.9.

For example, the Government must surely bear in mind the effect that its proposals for responding to the *Marper* judgment could have on the income to be realised from its plan, in due course, to sell some or all of its equity investment in the FSS. More generally, for those who piloted the introduction of current arrangements was there a risk of seeking to demonstrate professionally what could be done when, exceptionally within the forensic sciences, resources were available rather than delay this for greater deliberation about governance and proportionality? In any case, would the political climate have allowed such a pause?

- 1.12. The *Marper* judgment - partly as a result of timing with an impending General Election - increased the political significance of the debate by placing the Government under a legal obligation to reform the laws governing the retention of forensic bioinformation. This obligation has required the Government to review and justify its forensic bioinformation policies as well as explain some of the assumptions underlying them. The judgment itself draws heavily on arguments and analysis developed during this emergent discourse, particularly the report published by the Nuffield Council on Bioethics (NCOB), whose authority it specifically acknowledges. This vindicates the constructive and principled criticism of current DNA law and usage to ensure that the inadequacies in these arrangements are acknowledged. It did not mean, however, that the issues and recommendations for change elucidated over the years would be reflected in new legislation. A linear progression from the principles expressed in, for example, the NCOB report and subsequently endorsed at Strasbourg to the enactment of new legislation at Westminster was not guaranteed. The reason for this was explained by The Joint Committee on Human Rights:

‘... judgments of the European Court of Human Rights leave a considerable amount of discretion to the State concerned as to precisely how it amends its law, policy or practice to meet these obligations. The process of implementing a judgment of the European Court of Human Rights is therefore an unavoidably political process, constrained by the legal obligations (to stop the breach, provide a remedy for the individual concerned and to prevent new or similar breaches), but a political process nonetheless.’¹³

¹³ Joint Committee on Human Rights (2010), *Enhancing Parliament's Role in relation to Human Rights Judgments*, Fifteenth Report of Session 2009-10, HL 85 & HC 455 (London, The Stationery Office), para.15.

- 1.13. The force of this observation is demonstrated in the nature of the Government's legislative proposals and how they got through Parliament despite weaknesses in its claims exposed by well argued opposition and the scepticism of experts. Despite a long period of consultation and deliberation, the Government's draft legislation was published within months of a General Election. They were a disappointment to those who hoped for a more considered response to the *Marper* judgment or a greater willingness to work towards a degree of consensus while the draft legislation was before Parliament. Consequently, it is likely – irrespective of the passage of the Crime and Security Act 2010 - that the outcome of these debates will not be settled until the next Parliament unless the present Labour Government returns to power with a working majority or, if a minority government can rely on a coalition of supporters to block further reform. Such an outcome would only endure in the opinion of many authorities (see below) until the new retention legislation has been referred back to ECtHR.
- 1.14. The Bill contained some concessions for critics. An unequivocal change is that the deletion of volunteers' profiles has been brought into line with Scots law: consent may be withdrawn at any time.¹⁴ The effects of some other changes are less clear-cut. The Government initially proposed that there should be a legal duty of deletion where, in the judgment of the relevant chief constable, a DNA profile was obtained because a person was arrested as a result of, for example, mistaken identity or unlawful action by the police.¹⁵ During the Commons stage of the Bill, because of disquiet about current inconsistency in decisions concerning the deletion of data, the Government tabled amendments to centralise decision making, placing responsibility for 'guidance' with the NDNAD Strategy Board.¹⁶ However, it is unclear how these different and potentially contradictory provisions will work in practice, although another Report stage concession demanded that the Board itself be subject to limited Parliamentary scrutiny.¹⁷ Also, not all questions raised about how the new arrangements will work have been addressed. At present when a DNA profile is deleted from the database information relating to the profile is also removed from the PNC. This second deletion does not appear to be guaranteed by the arrangements in the new legislation.¹⁸
- 1.15. An even more startling lacuna in the Act is that, despite provisions to have cautions, and also reprimands and warnings under the Crime and Disorder Act 1998 treated as the equivalent to a conviction for the purposes of permanently retaining bioinformation, there appears to be no provision to reverse permanent

¹⁴ See the Crime and Security Bill as introduced into the House of Lords, clauses 14 (2) in respect of the amendment to PACE by the insertion of clause 64ZL

¹⁵ Hansard 18 Jan 2010, Column 34: See the Crime and Security Bill as introduced into the House of Lords, clauses 14 (2) in respect of the amendment to PACE by the insertion of clause 64ZL.

¹⁶ Hansard, 8 Mar 2010, Column 65: See the Crime and Security Bill as introduced into the House of Lords, clause 23 (2)-(3).

¹⁷ Hansard, 8 Mar 2010, Column 118: see the Crime and Security Bill as introduced into the House of Lords, clause 23 (4) and (6) which do not however, give Parliament any powers to vote on NDNAD governance rules.

¹⁸ Public Bill Committee, 26 January 2010, Q137 www.publications.parliament.uk, accessed 24 March 2010.

retention triggered by a conviction where that conviction has been quashed on appeal.¹⁹ There were a total of 1019 convictions overturned on appeal between 2000 and 2005 in the Court of Appeal (Criminal Division), with 439 successful appeals against conviction in 2009 alone. In addition, in Crown Courts hearing appeals from the Magistrates Courts, there were 3,651 appeals allowed in 2005, meaning that this is not an insignificant oversight.²⁰

- 1.16. Limitations in the information provided, and the time for debate available to parliamentarians meant that some questions could not be followed through. These included issues raised several times at the Commons Report Stage about the greater risk of adventitious matches as databases are enlarged or information is exchanged under the Prüm Treaty, particularly with countries using a different multiplex to the SGM+ multiplex used in the UK. There were also concerns expressed about whose DNA would be made available under the Treaty to other countries. Moreover, claims of 'national security' will impose the indefinite retention of the samples of unconvicted persons on Scotland. This will be wholly at the discretion of Scottish chief offices of police. This provision undermines the principle in that jurisdiction where retention, in the absence of a conviction, had hitherto always been subject to procuratorial or judicial review.²¹
- 1.17. The core political controversy and the key subject of debate at all stages, however, remains that of the circumstances under which a DNA profile might be retained in the absence of a conviction. The issue has to be addressed because of the *Marper* judgment: how the law governing this might be revised so that such arrangements are no longer 'blanket' and 'disproportionate'. The Government first proposed to keep such data for up to 12 years,²² but it finally elected for a six year retention period in most cases involving the arrest of an adult. The Conservatives propose similar arrangements to those in Scotland where retention is determined by the charge for which a person arrested, is normally limited to three years and in all cases is subject to procuratorial or judicial review.²³ The Liberal Democrats advocate that no profiles should be retained in the absence of a conviction.²⁴
- 1.18. During the Commons Report Stage both Opposition options, especially the former, were commended by the Chairman of the Police Federation, as more likely to maintain public confidence, in preference to the Government's proposals.²⁵

¹⁹ 2010 c. 17 is not any easy piece of legislation to read, but no account appears to be taken in the relevant sections, that is s. 14 (2) 64ZD (destruction of data relating to a person not convicted) and 64ZI (equivalence to conviction definitions and the provision to delete e.g. where the arrest was unlawful)

²⁰ See <http://www.hmcourts-service.gov.uk/> for Court of Appeal statistics and <http://www.official-documents.gov.uk/document/cm69/6903/6903.pdf> for Crown Court statistics for 2005.

²¹ The Crime and Security Bill as introduced into the House of Lords, clause 16.

²² Hansard, 8 Mar 2010: Column 39.

²³ Hansard, 18 Jan 2010, Column 45-46.

²⁴ *ibid.* Column 60.

²⁵ Public Bill Committee, 26 January 2010, Q39-49.

Ministers argued repeatedly that those proposals alone, even compared with the Scottish legislation (hinted at as a possible solution by ECtHR), reflect an evidence based approach. This claim was not validated by the President of ACPO, however, who instead suggested that six years is 'reasonable' or 'about right' for reasons of 'simplicity' or 'professional judgment'.²⁶ ACPO also made it clear that their views were influenced by cost and a preference for IT solutions. ACPO witnesses advocated a simple rule to govern data deletion informed by the assumption that this would enable the process to be managed by algorithm. The Scottish system, with its emphasis on an examination of individual circumstances, 'was rejected because it would take up an inordinate amount of police resources'.²⁷ They were not questioned about why, in a country where expenditure on law and order, as a percentage of GDP, exceeds that in any other G8 member state and two-thirds of this money is spent on policing, the options were so limited.²⁸ The House of Commons Home Affairs Committee, having studied the material published in support of the Government's claims, could only refer to the 'complexity of the issues' and 'conflicting evidence'. Nevertheless, there was cross-party agreement within the Committee that, in the absence of conviction, there is not a case for the retention of a DNA profile for more than three years and that research was needed to evaluate the forensic use of DNA.²⁹

- 1.19. MPs and The Joint Committee on Human Rights noted a Government Minister's statement: "We have obviously considered the [*Marper*] judgment and how far we can push the boundary of the judgment in relation to our wish to have protection for the public". The Joint Committee found such a 'very narrow approach' in order 'to maintain the main thrust of its original policy on the retention of DNA' unacceptable, and likely to result in a further successful legal challenge.³⁰ The latter view was shared by the Equality and Human Rights Commission. It wrote to all MPs to advise them that the Government's proposals would be in breach of Article 8.³¹ This is consistent with views expressed by the Secretariat of the Council of Ministers of the Council of Europe. It has opined that the automatic period of six years proposed by the Government would not comply with the *Marper* judgment.³²

²⁶ *ibid*, Q112-117.

²⁷ *ibid*, Q93 and 97-100.

²⁸ Soloman, E., Eades, C., Garside, R. And Rutherford, M. (2007) *Ten Years of Criminal Justice Under Labour: An Independent Audit*, London: The centre for Crime and Justice Studies at Kings College London, available at www.kcl.ac.uk/ccjs pp. 18-23

²⁹ Home Affairs Committee (2010), *The National DNA Database*, Eighth Report of Session 2009-10, HC 222-1 (London, The Stationery Office), especially paras 35-37.

³⁰ The Joint Committee on Human Rights (2010), *Legislative Scrutiny: Crime and Security Bill; Personal Care at Home Bill; Children, Schools and Families Bill*, Twelfth Report of Session 2009-10, HL Paper 67 and HC 402 (London, The Stationery Office), paras 1.8 -1.10 and 1.72.

³¹ Hansard, 18 Jan 2010, Column 37.

³² Public Bill Committee, 26 January 2010, Q149-150; the Secretariat statement is quoted in The Joint Committee on Human Rights (2010), *Twelfth Report of Session 2009-10*, HL 67 & HC 402 (London, The Stationery Office) at para. 1.47 and note 47.

1.20. The Government's reluctance to materially change its policy was expressed in a claim made by the Home Secretary. In the mandatory statutory statement about the compatibility of the provisions of the legislation with the ECHR, while accepting that the taking of fingerprints and samples is likely to constitute an interference with a person's right to a private life under Article 8, he went on to cite in aid of his claim, that the interference with a person's physical integrity is short-lived and could be characterised as 'minimal' - the House of Lords *Marper* judgment.³³ As The Joint Committee on Human Rights commented:

'... the reasoning of domestic courts may still be relevant even after a decision of the European Court of Human Rights, but we would sound a note of caution about the Government's continued reliance on the House of Lords judgment: the Grand Chamber's decision took account of the decision and reasoning of the House of Lords and came to a different conclusion about the ambit of the right to private life in Article 8 ECHR and what constitutes an interference with that right, and the Government cannot now rely on the House of Lords decision to the extent that it is inconsistent with the decision of the European Court of Human Rights.'³⁴

The Home Secretary's statement was matched by a different form of denial by one MP, Mr Cash. He did not acknowledge the importance of the domestic discourse that gave rise to and influenced the ECtHR judgment, and how this had reversed previous failures domestically to give these important and complex issues serious and consistent attention. Instead he criticised the employment of 'abstract principles that are decided in European Courts' in matters that 'could just as well have been decided' by English courts on the basis of UK legislation'.³⁵

1.21. This brief analysis of the recent political process at Westminster does not, of course, address the wider political considerations that, for the present at least have proved to be the decisive factor. The temptation to seek party political advantage from recent events was demonstrated by former Prime Minister Blair. In a carefully choreographed intervention in the pre-General Election campaign he asserted:

'On law and order the Tories.... even want to restrict the use of the DNA database. This employs the advanced technology of DNA tracking and matching, to provide incontrovertible evidence of guilt or innocence. Its use so far has resulted in extraordinary breakthroughs..... Yet the Tories oppose it.'³⁶

³³ Crime and Security Bill, Explanatory Notes (referring to the Bills introduced in the House of Commons on 19 November 2009), para. 216.

³⁴ *op.cit.* n.30, para. 1.20

³⁵ Hansard, 8 Mar 2010, Column 63

³⁶ The Guardian, 'Tony Blair election campaign speech – full text' accessed on 31 March 2010, at <http://www.guardian.co.uk/politics/2010/mar/30/tony-blair-election-campaign-speech-in-full> .

- 1.22. This partisan and, many would say, misleading exploitation of the issue for electoral advantage was echoed by the Prime Minister. Standing alongside the mother of a murder victim, he sought to convey the impression that the ability to detect the killer would have been frustrated by anything less than the Government's proposals. The foreword to a Home Office consultation document issued previously had also implied that the change required as a result of the *Marper* judgment might 'undermine a system that helped trap the [killer of Sally Anne Bowman]'. In fact, the procedure under which Ms Bowman's killer was detected, following the arrest of the perpetrator for a minor offence following which he was linked to the crime scene after his DNA was speculatively searched, was not affected by *Marper*. This had been raised with the Government as early as August 2009. The Prime Minister's assertions were challenged by both Liberty and the Liberal Democrats who were at pains to stress that they had not advocated changes in the use of speculative searching on arrest.³⁷
- 1.23. These tactical political manoeuvres need to be seen in the context of a General Election where the Government was judged by most commentators to be unlikely to win. A much greater problem that is currently systemic within English politics remains to be addressed whenever the recent legislation is revisited. As the then European Human Rights Commissioner, Signor Gil-Robles, observed in 2004 and anticipating the Government's 'push the boundary of the judgment' philosophy: 'The United Kingdom has not been immune... to a tendency increasingly discernable across Europe to consider human rights as excessively restricting the effective administration of justice and protection of the public interest....'³⁸
- 1.24. Some commentators have ascribed this to the reaction in the United Kingdom to the events of 11 September 2001. The British Government has attempted to curb civil liberties and reduce the transparency that should be the hallmark of a democratic government, not always successfully, despite periodically keeping the unease prompted by terrorism 'at a certain pitch'.³⁹ Other writers have noted this as a consequence of growing support for a more communitarian political ideology. Wilson for example, has compared Labour's response when it came to power to the sweeping economic and social changes under the previous Conservative administration. Because government had ceded much of their power over the economy, there was a greater disposition to intervene much more in the minutiae of national life. One of its primary tasks became that of making neighbourhoods safe.

³⁷ For warnings against the misuse of this case see: for example, see Northumbria University Centre for Forensic Science (2009), *Response to the Home Office consultative document 'Keeping the Right People on The DNA Database: Science and Public Protection'*, Engineering and Information Sciences, and the School of Law of Northumbria University, p.5. For more recent criticism by Liberty and the Liberal Democrats see: BBC, DNA database debate is 'confused', http://newsbbc.co.uk/z/hi/uk_news/politics/election_2010/8611278.stm .

³⁸ Wilson, B. (2009) *What Price Liberty?* London, Faber and Faber, p. 319.

³⁹ Grayling, A.C. (2008) *Towards the Light*, London, Bloomsbury, pp. 262-269.

- 1.25. The Labour Government was also greatly influenced by the private sector's apparent success in using information technology to improve effectiveness, for example, in anticipating and influencing consumer demand through 'dataveillance'. The ultimate goal of many key policy initiatives – in health, child protection, revenue collection and crime prevention, over the next decade therefore, had been the convergence of data to make possible speedy and cost-effective intervention, including pre-emptive action, by a smaller and more distant state. If Wilson is correct in this analysis and that privacy is 'a significant barrier to data-sharing, strategic-pre-emption and resource allocation, something which the government felt made it less powerful than private business',⁴⁰ the Government's reluctance to concede greater changes in response to *Marper* becomes more intelligible.
- 1.26. The Government is undoubtedly correct in recognising that the parameters for any debate about rights have changed. Dataveillance is a fact of everyday life, not least for academics with a Google dependency and for a younger generation that may respond to the frequent impersonality of modern life by exposing the private spheres of their lives to casual strangers in a way unacceptable to older generations. It would be wrong however, to seek to diminish the validity of a rights based discourse: it is difficult to identify a more defining characteristic of a law observing state. Hopefully the period when statements were made about how crime and terrorism 'mock' a system, built not for another decade but another age,⁴¹ has passed. Moreover, there is now a shared awareness in the political parties and some law enforcement interests, such as the Police Federation, of the need to rebuild public confidence. Indeed, this is the single national performance target for the police set by the Home Office. Possibly there is room for convergence between the Government and its critics on the basis of ideas developed in the field of bioethics for examining how citizens place trust in others and institutions.⁴²
- 1.27. In this report therefore, with the concern to secure public confidence and trust as our ultimate aim, we have attempted to systematically review the issues of evidence, and the significance of international exchange, along with some inter-UK comparisons in order to consider a variety of technological claims and foreseeable developments. We also seek to illuminate the range of current and emerging governance issues that need to be addressed. In doing so we hope that this will prove to be a measured and disinterested, albeit modest, contribution to the debate about the future of bioinformation that has already been joined at Westminster, but - as we anticipate at the time of writing - is quite possibly likely to be resumed during the next Parliament.

⁴⁰ *op.cit.* n.38, pp.317-337.

⁴¹ Downing Street Press Briefing, 15 May 2006; quoted in Wilson, B. (2009) *op.cit.* n.38 p. 351.

⁴² O'Neill, O. (2002) *Autonomy and Trust in Bioethics*, Cambridge, CUP.

Method

- 1.28. This project began with a review of the academic literature on forensic bioinformation, alongside a reading of annual reports of key agencies and documents produced by bodies that have considered the application of forensic bioinformation innovations to the criminal justice process in England & Wales. Following this work, a series of key issues was identified and summarised. These summaries were then used to support four meetings of law enforcement professionals, practitioners, government representatives, academics and other key stakeholders.
- 1.29. Each of three seminars began with scene-setting by the investigators with the remainder of the day dedicated to open (directed) discussion and debate. Finally, an international symposium provided an opportunity to test and further refine these ideas with relevant academic, policing and scientific experts from beyond the United Kingdom, including individuals working in European, North American and Asian criminal jurisdictions. The seminars were held on 13 January 2009, 25 March 2009, and 13 May 2009. The international symposium was held on the 28th and 29th of July 2009. Further details on all of these meetings can be found on the project website at: www.law.leeds.ac.uk/research/projects/bioinformation.php .
- 1.30. Experts working in specific domains of technological innovation have much to contribute to the wider social debates that surround their work. However, their views have not often been the subject of direct research.⁴³ This is certainly the case for those working within forensic bioinformation. In the course of this report we draw on the many dialogues that were occasioned by these meetings. We do not identify the contributions of individuals, as all discussions were held under the Chatham House Rule, but seek instead to represent a variety of expert views expressed by those with differing scientific, legal, policing and policy perspectives.
- 1.31. The critical examination of such practices that we present in the following pages, informed by the operational and policy perspectives of a large number of seminar and symposium participants, is largely focused on England & Wales, but also draws on international experience where that seems especially relevant. It pays particular attention to policy issues which are currently unresolved or contested and suggests how informed debate can be taken forward. It aims to identify those features of the present system and potential future developments, both nationally and internationally which either merit encouragement or give rise to concern.

⁴³ 'The views of experts have not been sufficiently evaluated, however, even though... they play an important role in shaping future practice.' Capron *et al*, 'Ethical Norms and the International Governance of Genetic Databases and Biobanks: Findings from an International Study.' (2009) *Kennedy Institute of Ethics Journal*, 19 (2) 101-124, p.101.

Report Themes

1.32. Several major themes emerged from reading the written material prior to the meetings and from the deliberations of participants in the meetings themselves. They are summarised in the three bullet points that follow.

- **Evidence and assessment.** A recent review of the NCOB report noted that: “A leitmotif in the report is the emphasis on further, more detailed evidence. Sound ethical advice and good governance depends upon solid facts and data.”⁴⁴ Insufficient research and the unsatisfactory way in which, sometimes, case studies and data have been presented means it is difficult to see how the bodies set up to utilise and oversee the NDNAD and IDENT1 can give adequate consideration to possible reforms unless this deficiency is addressed. There is little statistical evidence or rigorous comparative analysis of the facts in individual cases to show how and why forensic bioinformation is useful and to what extent is cost effective in either inceptive or probative terms. There is scant evidence about the costs of retrieving bioinformation in terms of individual cases.
- **Internationalisation and Exchange.** The international utilisation of forensic bioinformation and law enforcement co-operation is a growing consideration for those who think about the future of forensic bioinformation. Initiatives such as the Prüm Treaty are being implemented to facilitate the exchange of data for law enforcement purposes. Such exchange raises important practical questions for investigators and technical questions for scientists, but also issues of the cost-effectiveness and affordability of these initiatives. There are also questions to be asked about the harmonisation of different bioinformation systems and the possibilities of uniform processes across myriad jurisdictions with differing policing and judicial systems.
- **Governance and Accountability.** There is a need to demonstrate that reliable forensic bioinformation is being properly and consistently deployed, both within domestic policing priorities policies and practices, and also within emerging international systems for criminal investigations, surveillance (intelligence gathering) and control over the movement of persons. Consideration needs to be given to the requirements for ‘good’ (effective and ethical) governance of this socio-technical domain. This includes the future ‘steering’ of forensic bioinformation policies as well as current management. Issues such as the facilitation of transparency and accountability mechanisms, including the new demands of emerging counter-terrorism policies, all need further examination.

⁴⁴ Dierickx, K, ‘A Belgian Perspective’ (2008) *Biosocieties*, 3, p.97.

2 The Current Context

The Legal context

- 2.1. The police have had powers to take fingerprints of convicts since the 1891 Penal Servitude Act first provided for the measuring, photographing and fingerprinting of convicted prisoners,⁴⁵ although a warrant from a Magistrate was then required to take fingerprints from those on remand and if discharged, the prints were required to be destroyed.⁴⁶ It was not until 1948 that the Criminal Justice Act permitted the fingerprinting of suspects, although these still required a warrant from a Magistrate and were destroyed if the person was subsequently acquitted or not committed for trial. The Police and Criminal Evidence Act 1984 (PACE) introduced powers for the police alone to regulate the taking of fingerprints (terrorism, as well as immigration legislation, have also conferred powers on authorities to take fingerprints from individuals).⁴⁷ The power to take DNA samples was included in PACE, and sit alongside those powers to take fingerprints (and photographs), the powers being identical. PACE has been amended several times to facilitate the taking, use and retention of forensic bioinformation from widening categories of persons.
- 2.2. Fingerprints and DNA will ordinarily be taken with consent, but PACE also gives police the power to take samples without consent where the person has been arrested for, convicted of, or given a warning, caution or reprimand in respect of a recordable offence or told that he will be reported for one, or is answering bail at a police station and there is some doubt over identity,⁴⁸ or if they are detained following acquittal on grounds of insanity or finding of unfitness to plead. An officer must inform the person that their fingerprints/DNA will be subject to a speculative search (s61(7a)). PACE also preserves the power of compulsory fingerprinting contained in immigration and terrorism legislation while s27(3) gives the police the power to request someone to attend the police station to be fingerprinted, with a power of arrest for the purpose of taking fingerprints for a recordable offence.⁴⁹
- 2.3. The DNA database was set up, without dedicated primary legislation, in 1995.

⁴⁵ Regulations for the Measuring and Photography of Criminal Prisoners, SR & O 1896/762. This provision being continued by the Prison Act 1952 ss16 and 54(3).

⁴⁶ Leigh, L.H. *Police Powers in England and Wales* (2nd edn.) (London, Butterworths, 1985) p.228.

⁴⁷ See Terrorism Act 2000 Schedule 8 Part I s10; Anti-Terrorism, Crime and Security Act 2001 s89 (ss201); Asylum and Immigration Appeals Act 1993 s.3; Immigration and Asylum Act 1999 s141.

⁴⁸ Authorisation can only be given for the purposes of identification if the person refuses to identify themselves or the court, or an officer of at least the rank of inspector, authorises them to be taken if there are reasonable grounds for believing that he is not the same person; or the person who has answered to bail claims to be a different person from a person whose fingerprints were taken on a previous occasion.

⁴⁹ A recordable offence is one that can attract a custodial sentence upon conviction, however it also includes other offences that do not, including begging, selling alcohol to a person who is drunk, public drunkenness, and running onto a football pitch for example. The full list of recordable offences is found in National Police Records (Recordable Offences)(Amendment) Regulations 2005 (SI 2005/3106).

The power to speculatively search the database was provided for by an amendment to PACE in the Criminal Justice and Public Order Act of 1994, permitting DNA profiles and fingerprints to be speculatively searched against one another and crime scene profiles/prints. The powers to take and retain DNA (and therefore expand bioinformation databases) were significantly extended in 2001, and again in 2003, by removing the requirement to destroy profiles where there was no subsequent conviction, and expanding sampling powers so that the police could take fingerprints and DNA at the point of arrest, rather than when individuals were charged with offences. Section 64 of PACE then permits samples to be retained:

“after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person or of the person from whom a body part came.”

- 2.4. There remain additional powers to take and retain fingerprints under terrorism and immigration legislation. Most recently there has been an additional power to take DNA from people under ‘control orders’ which can be searched against law enforcement databases. In a change under the Counter-Terrorism Act 2008, s.14(5)(a) samples may now be used “in the interests of national security” in addition to those purposes detailed in PACE s.64. The Act also permits covert sampling, with the seizing of bioinformation without the knowledge of individuals who may be under surveillance. These samples are not necessarily held on NDNAD though they are retained, (it is not clear where), raising serious questions over the (separate?) governance of these samples. The Crime and Security Act 2010 permits 2 year extensions of retention for anti-terrorism purposes, which can be repeated. The Counter-Terrorism Act 2008 also includes provision for the use of DNA for the identification of an individual (not just bodies or body parts as under PACE 1984). This is a significant departure from the powers in PACE, and may have implications for human rights.
- 2.5. In the latest government proposals (detailed later) – measures were introduced to keep volunteers off the NDNAD – with reference to a ‘separate process’ for volunteers. However, no details were forthcoming about the nature of the separate process or of its regulation and oversight, and the Crime and Security Act 2010 permits the withdrawal of volunteers’ consent but provides no further detail on how this is to be managed. As yet – there is no agreement on who is a ‘volunteer’ as presently there are a variety of categories (police register volunteers; sex offenders; individuals worried about honour-based violence; missing persons etc.). In the case of fingerprints, there is a separate ‘elimination database’ for volunteers and a ‘special case’ facility, both of which are managed differently.

Crime and Arrest Rates

- 2.6. England and Wales, like much of Europe, has experienced a drop in recorded crime levels from the early 1990s. More recently, since 2004/05, the annual total of crimes recorded by the police has been falling, reaching approximately 4.9 million crimes in 2007/08.⁵⁰ However, despite the drop in crime, the number of arrests annually has been rising. In 2007/08, there were 1,475,266 arrests (albeit a slight dip of 0.5% in the usual year on year rises). Nearly a quarter of all arrests (24%) result in a caution, and these cautions contribute significantly to the overall detection rate, which in 2007/8 was 27%.⁵¹
- 2.7. The standardisation of arrest criteria in 2005 make comparisons of arrest rates across years problematic. However, between 2002 and 2006 there was a rapid escalation in numbers of children and young people being arrested – a rise far greater than in the adult population, and most marked in the 13-15 age bracket.⁵² Many of these arrests, it is claimed, are for 'trivial' reasons, and some have asserted, most plainly the past Head of the Youth Justice Board, Rod Morgan, that many were arrested to reach police arrest 'targets' and that young people were increasingly being criminalised.⁵³

Fingerprints and IDENT1

- 2.8. Fingerprint evidence has been used in criminal investigations and judicial processes for more than a century, initially to confirm questioned identity, and subsequently to assist in the identification of individuals whose fingermarks were recovered from scenes of crime. Current legislation means that any person arrested in connection with a recordable offence in England, Wales and Scotland, can have their fingerprints and palm prints taken. The fingerprint images, along with nominal data, will be entered onto the national fingerprint database and linked to a corresponding arrest record which is entered on the PNC in England & Wales, or the CHS (Criminal History System) in Scotland.⁵⁴
- 2.9. Fingerprints were first automated nationally in England & Wales in 1987 and significant technological developments are still continuing. IDENT1 stores the fingerprint and palm print databases (as well as the footwear impression database), and uses an Automated Fingerprint Identification System (AFIS) to compare fingerprints held on the national fingerprint database with those database holding unidentified marks from crime scenes.

⁵⁰ <http://www.homeoffice.gov.uk/rds/pdfs08/hosb0708summ.pdf> .

⁵¹ Home Office, 30 April 2009 Statistical News Release: Police Powers and Procedures England and Wales 2007/08. Available at <http://www.statewatch.org/news/2009/may/uk-ho-stats-police-prel.pdf> .

⁵² Home Office Statistical Bulletins: "Arrests for Recorded Crime" 02/03 – 05/06.

⁵³ See Centre for Crime and Justice Studies, 'Summary Justice: Fast but Fair?' (August 2008). Available at <http://www.crimeandjustice.org.uk/summaryjusticefastbutfair.html> .

⁵⁴ Scotland removes these records on acquittal.

- 2.10. LIVESCAN electronic scanners linked to the National Automated Fingerprints Identification System (NAFIS) are also available in most police stations for almost instantaneous searching of fingerprints taken from individuals against the over 8 million sets of fingerprints held on IDENT1. Mobile scanners are also available for use on the street to search individuals against the Police National Computer. Earlier LANTERN hand held mobile fingerprint consoles are now being replaced, firstly under Project MIDAS ('Mobile Identification at Scene'), and now by the UK's 'National MobileID' service.
- 2.11. IDENT1 has been designed, developed, and is managed by Northrop Grumman Information Technology (until at least 2013), a contractual service which is overseen and controlled by the NPIA. This service is also increasingly used by the UK Border Agency for checking of biometric visas and passports and processing of visas. Up to 8,500 visa applications a day are anticipated to be using IDENT1 for identification in the near future, and IDENT1 is expected to play a crucial role in the creation of links with the Schengen SIS II, a European-wide searching system for law enforcement agencies.

DNA Profiles, Samples, and the NDNAD

- 2.12. DNA profiling has been used by the police to investigate crimes for over 25 years.⁵⁵ Despite some early and well-publicised difficulties in its acceptance by the Courts, especially in the United States, it is now more often portrayed as the standard-bearer of forensic science quality, with claims made for its unrivalled power to inculpate the guilty as well as exculpate the innocent. In order to facilitate the use of DNA profiling, and maximise its utility, the National DNA Database (NDNAD) was established in 1995, growing rapidly with the aid of legislative amendments extending police powers to take and retain DNA over subsequent years. There has also been significant financial investment in the technology. The history of the NDNAD, assisted by the comparatively greater openness of this database than other police or government bioinformation systems, has already been charted by a number of studies.⁵⁶
- 2.13. Until the recently passed Crime and Security Act 2010, there was no statutory basis for the governance of NDNAD. Upon establishment, it was initially operated and overseen by the Forensic Science Service. However, Custodianship is now in the hands of the NPIA, which was established by the Police and Justice Act 2006, commencing operations in April 2007. The NPIA is a police-led, central resource, governed by a tripartite arrangement – with the Home Office, the Association of Chief Police Officers (ACPO) and the Association of Police Authorities (APA). All NPIA work is overseen by a Board,

⁵⁵ The scientific background to forensic DNA profiling is described in a number of publications. A useful and short introduction may be found in Chapters 1 & 2 of the Nuffield Council on Bioethics: *The Forensic Use of Bioinformation: Ethical Issues* (September 2007).

⁵⁶ Williams. R. & P. Johnson, '*Genetic Policing*' (William Publishing, Cullompton, 2007).

which must ensure that they reach their aims and objectives and that they comply with statutory and administrative requirements for the use of public funds.⁵⁷ As with predecessors however, the NPIA is not immune to change or disbandment, with suggestions that the NPIA may be removed by a Conservative government and the recent announcement of the impending departure of the Chief Executive.

- 2.14. A 'full DNA 'profile' held on the NDNAD consists of the 20 numbers that are measured by the SGM+ multiplex, together with a sex marker (Amelogenin). Each number represents a measurement of the repeat frequency ('peak') for each of the two alleles at the positions or loci along the chromosome selected for analysis or typing as a DNA profile within the multiplex (sometimes called 'marker') kit or system. Thirty-six additional non-genetic data fields are available for each sample profile, although not all records will have entries for all 36 fields as this will depend upon their origin.⁵⁸ At the present time, the DNA 'sample' – the DNA extraction made from the cellular material provided by individuals or collected from crime scenes – is also retained by the processing laboratory on behalf of the police force that originally collected the material.
- 2.15. The NDNAD is linked to the Police National Computer (PNC), maintained and operated by the NPIA, and provided for by s.27(4) of PACE. Regulations made under that section also regulate the information that is to be kept, including details of people, vehicles, crimes and property. The PNC can be accessed by the police and other criminal justice and related agencies with approximately 185 million transactions during 2008. Transactions are currently growing by approximately 10% per year.⁵⁹
- 2.16. Changes to policy, requirements to keep data to support the retention of DNA and fingerprints, a recent Court ruling, and a failure to follow this issue through during the Commons Committee stage of the Crime and Security Act 2010 mean that records on the PNC are no longer 'weeded', and old or minor convictions, or arrests that do not result in a conviction (i.e. arrests with NFA) are 'stepped down' (i.e. not immediately accessible to non-police agencies), but are retained by the police and may be revealed on a 'standard disclosure' to non-police agencies. This has implications for all individuals who are arrested, as these records will remain permanently and being 'a person known to the police', may impact upon visa and job applications for example.

⁵⁷ NPIA Business Plan 2009 – 2010. p.15. Available at: <http://www.npia.police.uk/en/7403.htm> .

⁵⁸ For a description of all the data entry fields, see: Home Office, 'Keeping the Right People on the DNA Database' (May 2009).

⁵⁹ www.npia.police.uk accessed 1 December 2009.

Cost

- 2.17. Individual police forces pay their forensic provider (with whom they have a contract) for DNA testing. Each force must then budget for their needs and will spend varying amounts on DNA testing and associated activities (such as crime scene recovery). Fingerprinting may be harder to accurately cost as fingerprint bureaux are operated locally by each force. It has been commonly believed that because of this 'in-house' provision of fingerprint analysis, fingerprints are 'cheaper' than DNA testing, though this may not necessarily be the case or a particularly meaningful statement.
- 2.18. The cost of running the NDNAD, including the monitoring and accrediting of forensic DNA suppliers increases as the number of suppliers increases, though in recent years, some of this cost has been passed onto suppliers. However, there has still been an increase in costs, notwithstanding the one-off 2008/09 cost of the transition of the NDNAD operation from the FSS to the NPIA.⁶⁰ Maintenance costs are approximately £200,000 per annum while development costs for future years are yet to be publicly made available by the NPIA. The total cost of the NDNAD in 2008-09 was £4,290,500 (this includes both capital and running costs; it is not possible to separate the two, as well as almost £1m in costs relating to the transfer to the NPIA).⁶¹
- 2.19. The NPIA will not reveal the costs associated with IDENT1/ Livescan because it forms part of a private contract with Northrop Grumman and is therefore considered commercially sensitive. On this basis, the NPIA has claimed exemption from the right of access in accordance with sections 41(1) and 43(2) of the Freedom of Information Act.⁶² However, in 2004, it was reported that Northrop Grumman won a US\$244 million contract (approx. £125m at 2004 exchange rates) to provide advanced biometric identification technology to the UK police. The contract was for eight years with three additional option years, and followed the NAFIS contract that it held from 1995.⁶³ The NPIA recently awarded Detica an £18.1m contract to deliver an Automated Fingerprint Identification System (AFIS) to provide a nationwide mobile biometric identification capability through a selection of different hand-held devices.⁶⁴

⁶⁰ NPIA website, accessed on 1st December 2009.

⁶¹ Lord West of Spithead, Written Answers - HC Deb, 2 December 2009, c51W.

⁶² Section 41(1) exempts information if it was obtained by a public authority from any other person and the disclosure of the information would constitute an actionable breach of confidence. This exemption is absolute so does not require a 'public interest' test to be undertaken. Section 43 also exempts information if it is likely to prejudice commercial interests, although this is a qualified exemption, and the balance of public interest and the benefit to the community at large, should be considered before disclosing the information.

⁶³ Northrop Grumman Wins U.K. Fingerprinting Job, *The Washington Post*, December 20, 2004; Page E04.

⁶⁴ '\$25m mobile biometric ID deal awarded by UK's NPIA' *Biometric Technology Today*, March 2010, p.1.

The International Context

- 2.20. The Secretary General of Interpol has observed that the use of DNA on a significant scale has been restricted to a club of wealthier countries.⁶⁵ While this may remain true, the latest Interpol survey shows that over 50% of countries in all regions, except Africa, use DNA profiling in criminal investigations. There are 120 Interpol countries using DNA profiling and 54 of these have national DNA databases with 26 countries planning to introduce a DNA database.⁶⁶ The numbers of fingerprint databases across the globe are not detailed, but will likely be far higher, with the century of use and 'affordability' of fingerprinting.
- 2.21. International cooperation involving the exchange of DNA, however, is in its infancy. Information is scarce and despite publicity for some successful cases, cooperation appears to be far from regular procedure even for investigating serious crimes. Within the EU this might change as a result of the Prüm Treaty, although there is evidence to suggest that the introduction of technologically advanced searching systems and databases will not necessarily result in major increases in activity. Indeed, the Council of the European Union has already taken action to restrict the level of dactyloscopic searching under Prüm, presumably to prevent analysts being overwhelmed by additional searches. This in turn suggests that the amount of cooperation involving the use of fingerprints is much lower than is commonly imagined, but while information about the volume of UK involvement in international cooperation is rare, data about the exchange of fingerprint information appears to be non-existent.
- 2.22. There are various technical obstacles to greater international cooperation the most significant being the imminent technological obsolescence of the SGM+ multiplex. In contrast to the Government's earlier strategy for upgrade of profiles from SGM to SGM+, the absence of retained samples as a result of the Crime and Security Act 2010 may mean that retained profiles may frequently have little value for international comparison purposes well before the normal minimum six year retention period under that act expires.
- 2.23. The modest ambitions for enhanced criminal justice cooperation internationally are dwarfed by the anticipated scale of activity intended for the purposes of border control. Inevitably this will result in the vertical integration of searching systems and databases with criminal justice resources and operations. Potentially the amount of information held by the state, as a result of (quasi-) consensual access to bioinformation, could make existing arrangements based on forfeiture increasingly irrelevant, particularly as fingerprints and, possibly, DNA are used for border control purposes.

⁶⁵ Quoted in Wilson, T (2009) '*Forensic Science and the Internationalisation of Policing*' in Fraser, J. G. and Williams, R. (eds.) *Handbook of Forensic Science* (Cullompton: Willan Publishing), p.506.

⁶⁶ INTERPOL, *Global DNA Profiling Survey 2008, Key Facts*. Available at www.interpol.int.

3 EVIDENCE AND ASSESSMENT

Evidence and assessment

- 3.1. In the course of its deliberations on the legality of the UK forensic DNA collection and retention regime that has been in place since 2001, the European Court of Human Rights considered the quality of the evidence presented to the Court concerning the usefulness of the retention of DNA samples and profiles from those who, although arrested by the police, remained unconvicted of any crime. In its judgment, the Court observed that

“... the statistical and other evidence, which was before the House of Lords and is included in the material supplied by the Government appears impressive, indicating that DNA profiles that would have been previously destroyed were linked with crime-scene stains in a high number of cases.”

However, this seemingly impressive appearance did not withstand detailed scrutiny, and the Court concluded that:

“neither the statistics nor the examples provided by the Government in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position”.

The judges in this case were evaluating a very narrow range of claims made by the Government; that related largely to the usefulness of retaining forensic bioinformation from individuals who had not been convicted of criminal offences. Nevertheless, their comments, both here and elsewhere in their judgment, give pause for thought about the quality and quantity of evidence that currently exists concerning the effectiveness of the uses of bioinformation more generally. It is this issue that will be the focus of this section of the report.

- 3.2. The dismissive view of the Court surprised many key actors in the UK network of forensic bioinformation advocates and users, especially since strong claims about the usefulness of forensic bioinformation for the investigation of crime has been a constant factor in the UK policy debate. Early FSS estimates of the usefulness of the NDNAD for the detection and reduction of volume crime were undoubtedly influential in securing funding for the expansion of the NDNAD through increases in collection rates from subjects and crime scenes between 2001 and 2005.⁶⁷ The subsequent modification of the ‘FSS General Crime

⁶⁷ Although the DNA Expansion Programme was established in order to fund increases in the collection of DNA, it quickly became clear that the work of the new cadre of crime scene examiners employed through

Reduction Model' by the 'MHB Model' provided by the authors of the 'Pathfinder' study did not substantially change this optimistic view, and official statements concerning the NDNAD have further emphasised its significance to the detection of both volume crime and serious crime.⁶⁸ Assertions made in a key document that summarised the effectiveness of the Expansion Programme, especially those that favourably compared the overall detection rates for volume crimes to the detection rates when DNA crime scene samples were loaded onto the NDNAD, are frequently repeated in the UK and elsewhere in support of the establishment or expansion of DNA databases elsewhere in the world.⁶⁹ Whilst most such claims focus only on the detection, rather than the prosecution of offenders, the recent Magee Report suggested that "improved use of biometrics in prosecuting and convicting could lead to 1% more convictions of those tried at court."⁷⁰

- 3.3. However, alternative voices in the UK debate on forensic bioinformation have often argued that there is a need to improve the research base from which to launch any such assertions. The House of Commons Science and Technology Committee called for more research in their report '*Forensic Science on Trial*' in 2005, and it was also the view of the Nuffield Council on Bioethics, as cited by the European Court of Human Rights. This view has subsequently been endorsed by other authorities, including the Human Genetics Commission.⁷¹ A series of commentaries and papers by Genewatch, often in response to specific Ministerial statements, or as submissions to consultation exercises, have provided very detailed critiques of data quality as well as the credibility of the interpretations of existing data on the use of DNA profiles in criminal investigations offered by official spokespersons.⁷²

this programme would result in an increase in fingerprints as well biological samples collected from crime scenes.

⁶⁸ Both models are fully outlined in Burrows, J. et.al. (2005) *Forensic Science Pathfinder Project: Evaluating Increased Forensic Activity in Two English Police Forces*. London: The Home Office.

⁶⁹ See pages 16-17 of Home Office Forensic Science and Pathology Unit (2006) *DNA Expansion Programme 2000-2005: Reporting Achievement*. London: The Home Office.

⁷⁰ Sir Ian Magee, '*The Review of Criminality Information*' (The Magee Report) (July 2008) Home Office, London. p.17.

⁷¹ Statements to this effect can be read both in the HGC response to the Consultation Paper and, in more detail, in their 2009 Report: '*Nothing to Hide, Nothing to Fear*'.

⁷² A full collection of these papers can be found on the Genewatch website: <http://www.genewatch.org/sub-539478> accessed 16th April 2010.

- 3.4. Following the delivery of the European Court judgment, the UK Government commissioned additional work which sought to provide further evidence on the usefulness of retaining fingerprints and DNA profiles from those not convicted of crimes.⁷³ This work was explicitly used to support proposals for changes in the retention regime that would meet the Court's demands, but following its publication, the study was subjected to a series of critical commentaries. Its standing now remains unclear. Rather than engaging directly in this dispute we want briefly to outline the currently available official data sources on which any such evaluations can be based, as well as what can be learned from some of the existing academic studies of the police uses of forensic bioinformation.⁷⁴ In the course of doing so, we want to explain why so many observers find the existing data, and many of the current studies, wanting in the support they provide for an authoritative account of the effective uses of forensic bioinformation in criminal investigations and prosecutions. We begin by describing the different kinds of information that circulate in the public realm before offering a commentary on its quality and relevance.
- 3.5. The most basic level of facts relevant to understanding the operation of forensic bioinformation regimes in any criminal jurisdiction relate to the amount of such information held by relevant authorities together with other significant facts retained about the individuals whose biometric data have been captured for inclusion. We provide below some recent figures on the number of fingerprint and DNA profiles holdings in relevant databases in England & Wales.
- 3.6. According to the most recent statistics issued by the National Policing Improvement Agency, in October 2009, IDENT1 held:
- 8.1 million individuals' ten-prints
 - 17.8 million sets of ten-prints
 - 1.8 million unidentified marks
 - 7.9 million palm prints
 - 156,210 palm marks
 - 4,396 serious crime marks

It can be seen – from the figures shown in the next section – that the size of this collection is much greater than that of the current DNA database. This is of course an historical artefact resulting from the longer history of the collection of fingerprints from offenders and recovery of fingermarks from scenes of crime. However, it is important to note that the size of the fingerprint collection has often been used to anticipate the eventual size of the NDNAD, and since its

⁷³ Especially the study by Ken Pease appended to the Consultation Paper: *Annex C: DNA Retention after S and Harper*: Ken Pease, Jill Dando Institute. April 2009.

⁷⁴ Whilst our description of existing data sources are limited to those held in England & Wales, we also introduce some examples of recent research from other jurisdictions to indicate the kinds of studies that might be possible here in the future.

establishment in 1995, the collection of DNA subject samples and fingerprints from those arrested on suspicion of involvement in a criminal offence has been treated as an equivalent necessity. Accordingly, since that time and with some variation resulting from local arrangements, the number of new DNA subject samples loaded onto the NDNAD has been equivalent to the number of new tenprint records loaded onto the fingerprint database. At the same time, recovery rates of these two different forms of bioinformation from crime scenes remains very different: the number of fingerprints recovered from crime scenes remains considerably higher than the number of biological samples recovered, but the attrition rate is also much greater. In view of these facts it seems surprising that more efforts have not been made properly to assess the usefulness of fingerprints to crime detection, particularly as enhancing their value to investigators was one of the intentions of moving from the DNA Expansion Programme to the Forensic Integration Strategy.⁷⁵

3.7. The most recently available figures on the NDNAD⁷⁶ show that the database held the following:

- 5.6 million subject sample profiles
- 4.9 million (est.) individuals who correspond to those sample profiles⁷⁷
- 354 thousand unmatched crime scene sample profiles;
- 39 thousand sample profiles from volunteers.⁷⁸

In recent years, approximately 50,000 subject samples have been loaded onto the NDNAD each month. Crime scene profiles are deleted from the NDNAD at the request of the police following a conviction for the offence or when a decision is made that it will not be investigated further. Between 2007 and March 2009, 52,688 crime scene profiles were removed from the NDNAD.⁷⁹

3.8. Individuals who wish to have their profiles removed from the NDNAD must make their request to the Chief Constable of the force who obtained their DNA. Between March 2007 and March 2009, 445 subject profiles were deleted from the NDNAD under the 'Exceptional Case Procedure.' However, the law regarding DNA retention differs in Scotland so during the same period, 35773 Scottish subject profiles were deleted from the NDNAD.⁸⁰

⁷⁵ Home Office (2006), *DNA Expansion Programme 2000-2005: Reporting Achievement*, London, Home Office, p. 20.

⁷⁶ Taken from NPIA website, accessed on 1st December 2009.

⁷⁷ It is currently estimated that as at 16 October 2009 13.8% of the subject profiles held are replicates.

⁷⁸ These figures do not include sample profiles held on the Police Elimination Database (PED). PED searches are carried out only if a senior investigating officer requests a comparison of profiles from a specified officer or officers with a DNA profile from a specified crime, unlike NDNAD searches which compare all profiles from crime scenes with all profiles from known individuals. Since 1 August 2002, all new recruits to the police service have been required to give a DNA sample as a condition of employment. As at 30 September 2009 there were 118,699 records held on the PED for England and Wales police forces.

⁷⁹ NDNAD Annual Report 2007-2009, p.25.

⁸⁰ *ibid.* p.25.

- 3.9. On 24th April 2009 there were an estimated 986,185 persons included on the NDNAD who had no conviction recorded on the PNC either because their PNC record has been 'weeded' and has therefore been deleted, or because proceedings against them are still ongoing, or because or they have never been convicted of an offence.⁸¹ These subject profiles without corresponding PNC records are often confusingly referred to as 'innocent' people on the NDNAD although it is only the third of these groups that would correctly be called 'innocent' (and those in the second group are yet to be decided upon so may or may not join this group). We have already noted that the retention of this group of subject profiles is subject to considerable contestation, and we will return to discuss this group later in this section of the report.
- 3.10. It may seem intuitively obvious that the larger the number of profiles and fingerprints held in any forensic database, the more useful will be these holdings to the process of criminal investigation since they will eventuate in more matches and identifications. The rising match rate observed throughout much of the time that the NDNAD has grown, may seem to support this general idea, although there have been stutters in the upward trajectory. However, the most recent comparative data on DNA database sizes and match rates provided by ENFSI shows no simple association between the two measures,⁸² and it is likely that important determinations of such rates include the extent to which legislation and practice eventuate in the collection of bioinformation from the most relevant category of individuals, and the assiduousness with which biological material and fingermarks are collected from scenes of crime.⁸³ In addition, care has to be taken when comparing match rates between different DNA databases (and sometimes between the same database at different points in times) since match counting rules may differ.⁸⁴

Forensic Bioinformation: Existing Data Sources

- 3.11. IDENT1 is used to compare fingermarks at crime scenes with fingerprints held in the National Fingerprint Collection. Automated searching – and the candidate identification of crime scene marks with the fingerprints of individual suspects – is supplemented by expert evaluation and decision-making. The NDNAD is used to automatically compare crime scene profiles with profiles obtained from suspects for the offence in question as well as profiles obtained from individuals arrested in connection with a recordable offence. Some data are provided by

⁸¹ *ibid.* p43.

⁸² ENFSI (2009) DNA-Database Management Review and recommendations at http://www.enfsi.eu/get_doc.php?uid=345, accessed 6 March 2010. We later take up the issue of the relationship between match rates and the more difficult question of the significance of, and uses made, of such matches.

⁸³ Attentiveness to this categorical issue can be seen in the various descriptions of the population that the NDNAD was hoped to capture. These have included 'the active criminal population', 'the active known criminal population', and 'the known active suspect criminal population'.

⁸⁴ See comments on match counting rules for scene-to-scene matches in particular by Buckleton, Bright and Walsh (2009) 'Database crime to crime match calculation' *Forensic Science International: Genetics* 3: 200-201.

IDENT1 and the NDNAD on the number of identifications and matches that are provided to the police each year. Examples of these are shown below.

Fingerprints

3.12. From April to October 2009, IDENT1 made 47,783 crime scene 'identifications', averaging 85000 identifications a year. In addition, it verifies the identity of over 1.5million arrestees per year. There are no data on the number of identifications that led to detections or convictions. Presently, there are 2000 identity checks being processed via mobile devices per month, and the UK Borders Agency uses IDENT1 to check over 4000 identities per week.⁸⁵ However, no data are centrally provided from IDENT1 on the uses made of these identifications to support the detection or prosecution of offenders.

DNA Profiles

3.13. Crime scene profiles may 'match' with both subject profiles as well as with other crime scene profiles. Subject profiles can also match with each other.⁸⁶ In 2008-09, the average match rates between crime scene and subject profiles when a new crime scene profile was loaded onto the NDNAD was 58.7%; when a new subject profile was loaded it was 2.3%.⁸⁷

3.14. A 'match' refers simply to two profiles being found to match on the database. These will include cases where an individual whose DNA profile is found at a crime scene may have a legitimate reason for their biological material being present (e.g. they are a victim, a witness, or otherwise legitimately present). In such instances, there will be no 'detection' resulting from the match. A 'DNA detection' refers to cases where a crime has been cleared up and a DNA match was available to investigators. However, such 'DNA detections' cannot be assumed to have resulted from the DNA match itself. A supplementary category of 'Additional DNA detections' includes cases in which an offender being presented with his DNA 'match' for a case, then admits to further offences.⁸⁸

3.15. 'Multiple matches' also occur in cases where a crime scene matches with more than one subject profile. Such multiple matches normally arise because a partial crime scene profile matches against a number of full subject profiles or because the same person's profile is held on the NDNAD under different names (a replicate). Between May 2001 and March 2009, 306,379 crime scene profiles have been identified in 282,861 match groups.⁸⁹ For 226,393 of these, a single subject was reported as linked to the crime scene by their DNA.⁹⁰

⁸⁵ NPIA Business Plan 2009-2010, p.31.

⁸⁶ In the case of 'replicate profiles'.

⁸⁷ NDNAD Annual Report 2007-2009, p.33.

⁸⁸ *ibid.* p.35.

⁸⁹ *ibid.* p.28. A 'match group' consists of two or more DNA profiles that are indistinguishable or compatible.

⁹⁰ *supra.*

- 3.16. Since 1995 (until March 2009) 556,794 crime scene profiles have been loaded onto the NDNAD and during the decade 1998/99 to 2008/09 there have been 410,000 crime scene to subject matches, which may have been useful to the investigation, if not directly identifying the offender. In 2008/09, there were 36,727 matches between crime scene and subject profiles, of which 17,607 led to DNA detections, and 14,602 'additional' detections, a total of 32,309 crimes detected in 2008/09 in which a DNA was available.⁹¹ While taken as a proportion of the number of crimes reported (approx. 4.9 million), this number is very low, yet there are proportionally few crimes where there are 'scenes' that can be usefully searched, and many other factors that will preclude the use of DNA evidence (including in most instances all those involved already being identified). In 2008-09, just 796,780 crimes were subject to a crime scene examination (17% of recorded crimes), meaning approximately 2.21% of all examined crime scenes led to DNA detections in 2008/09.⁹²
- 3.17. There are very considerable difficulties in interpreting the significance of these kinds of figures provided by the NDNAD when attempting to assess the general usefulness of genetic forensic bioinformation for the investigation of crime. Ministers have frequently used answers to Parliamentary Questions to provide seemingly better summary data, but even here, the same difficulties recur. In the following paragraphs we consider one example of such a House of Commons answer in order to illustrate these issues. In this case, the Secretary of State for the Home Department provided a table of results (shown as Table 3.1 overleaf) to the House of Commons on 25th January 2010 (HC 642W).
- 3.18. The written statement includes a number of claims, caveats and explanatory notes to the table. Perhaps the most important of these is the assertion that the data in the table 'under-represent the overall contribution of DNA matches to the detection of serious crimes such as murder and rape.' The reason for this is that the figures for detections do not include those cases in which 'one-off speculative searches of the NDNAD' played a part in a successful detection, nor do they include those cases in which only laboratory-based DNA profile comparisons were deployed. The former are usually carried out when crime scene profiles are insufficiently complete to be suitable for NDNAD loading, and the latter are carried out without the direct deployment of the NDNAD. The Secretary of State also asserted that these DNA routines are deployed more commonly in serious crime investigations and it is the neglect of these that may result in an under-representation.
- 3.19. However, since no data are provided on the number of such comparisons, it is obviously difficult to assess their effect on the overall picture provided. Other caveats included in the written answer include the standard remark that

⁹¹ NPIA website accessed on 1st December 2009.

⁹² NDNAD Annual Report 2007-2009, p.27.

'detections are achieved through integrated criminal investigation, not through DNA alone', but it is interesting to note that in this instance, the usual preceding modifier 'serious crime' has not been used. Finally, it is noted that 'The data provided are management information and have not been formally assessed for compliance with the Code of Practice for Official Statistics.' The statistics have been compiled from individual police forces' forensic performance data, albeit standardised data collected according to Home Office pro-forma'.

Table 3.1

<i>DNA-related detections 2008-09</i>							
<i>Police forensic data-2 crime categories</i>	<i>Detections of crimes in which a DNA match was available ('DNA detections')</i>	<i>Additional detections arising from the DNA match</i>	<i>Total DNA-related detections ('DNA detections' and additional detections)</i>	<i>Recorded crime 2008-09</i>	<i>Total force detections 2008-09</i>	<i>Total DNA-related detections as proportion of recorded crime (percentage)</i>	<i>Total DNA-related detections as proportion of total force detections (percentage)</i>
All other recorded crime	1,506	1,616	3,122	1,315,079	368,595	0.2	0.8
Criminal damage	2,886	896	3,782	936,729	131,442	0.4	2.9
Domestic burglary	3,702	4,015	7,717	284,445	46,500	2.7	16.6
Drugs offences	397	179	576	242,907	230,962	0.2	0.2
"Homicide" ⁽¹⁾	70	4	74	11,248	4,583	0.7	1.6
Other burglary	3,830	2,571	6,401	296,952	31,371	2.2	20.4
Other sex offences	106	34	140	38,355	12,760	0.4	1.1
Other violent offences	861	168	1,029	892,745	422,224	0.1	0.2
Rape	168	1	169	13,133	3,411	1.3	5.0
Robbery	603	148	751	80,104	16,816	0.9	4.5
Theft from vehicle	2,036	3,655	5,691	444,647	42,642	1.3	13.3
Theft of vehicle	1,298	1,165	2,463	147,470	24,471	1.7	10.1
Unknown	144	150	294	n/a	n/a	n/a	n/a
Total of 12 crime types	17,607	14,602	32,209	4,703,814	1,335,777	0.68	2.41

(1) The forensic data "homicide" crime category covers the following recorded crime categories:
Murder, Manslaughter, Infanticide-648
Attempted murder-575
Intentional destruction of viable unborn child-8
Threat or conspiracy to murder-9,559
Causing death by aggravated vehicle taking etc.-31
Causing death by dangerous, careless or inconsiderate driving-427
Total 'Homicide' crimes in 2008-09-11,248

Notes:
1. A 'DNA detection' means that the crime was cleared up and a DNA match was available.
2. 'Additional detections arising from the DNA match' occur when, for example, a suspect, on being presented with DNA evidence linking him to one offence, confesses to further offences. They arise from a crime with a DNA match; and are therefore detections where a DNA match played a part in solving the crime.
3. Total 'DNA-related detections' means 'DNA detections' plus 'additional detections arising from the DNA match'.

- 3.20. Some general observations on these data are in order. First, that the category of 'DNA Detections' (defined as detected crimes 'in which a DNA match was available') remains heterogeneous. The table gives no information about the role played in an investigation by the DNA match, although there are data fields on the relevant Home Office pro-forma which require some indication of the role played. Even without this information, it seems intuitively obvious that the availability of DNA matches in detecting 70 of the 4,583 homicides detected in 2008-2009 will differ according to the nature of the varied cases (including murder, manslaughter, infanticide, attempted murder, the destruction of a viable unborn, threat to murder, and causing death by dangerous driving, etc) and the dynamics of particular investigations.
- 3.21. Second, it should be noted that since the role of a DNA match in aiding the original detection remains unexplicated, it is difficult to know what significance to place on figures given in the adjacent column of 'Additional detections arising from the DNA match'. Without this, and despite the Government claim that since these detections 'arise from a crime with a DNA match; and are therefore detections where a DNA match played a part in solving the crime', it hardly seems necessary to add the concept of 'Total DNA-related detections', which combines together the first two categories, increasing confusion.⁹³
- 3.22. If these observations give some sense of the difficulty of reaching simple conclusions from these data, this difficulty is multiplied when questions are asked about the effect of the retention of particular categories of persons. Many such questions have been asked of Ministers in Parliament, but a brief survey of their replies indicates the level of ambiguity and imprecision that surrounds them.⁹⁴
- 3.23. Better summaries and analysis may be found elsewhere. For example, the ACPO Criminal Records Office (ACRO) recently has become involved in the analysis of existing data on behalf of the NDNAD Strategy Board. One of their recent studies determined that in 2008/09, there had been 818 subject profiles matched with homicide or rape crime scene profiles. In 82 of these matches, the subject did not have a prior conviction, and their DNA was matched when the crime scene profile was loaded. Senior detectives involved in these 82 cases reported that in 43 of them, the match was 'important', although the various meanings that may be captured by the use of this term remain open to

⁹³ There is one other major issue about these data: the use of proportions in the final two columns may be statistically inappropriate since figures for recorded crime and for detections relate to the same year, but not necessarily to the same data-set. Force detections achieved in the year 2008-2009 may include the detection of crimes recorded in earlier years, and crimes recorded in 2008-2009 may be detected in subsequent years. It is conventionally argued that this 'rolling proportion' remains roughly accurate, but it does not seem to represent good statistical practice. Once again it is something that can be corrected if and when proper case-tracking data become available for analysis.

⁹⁴ Once again, Genewatch papers can be consulted for the details of many of these.

speculation.⁹⁵ More recently, the government presented five case studies intending to demonstrate the power of retaining the DNA of 'innocent' individuals, in subsequently detecting further offences. Of these five however, two were the same case, and of the four remaining cases, one of the rapes occurred inside the suspect's bedsit, and a burglar had recently been dismissed from employment at the burgled premises and he had been caught on CCTV, leaving the studies lacking much persuasive force.

Police Force Returns

- 3.24. Is it possible to develop a better grounded understanding of current police uses of forensic bioinformation through the analysis of locally collected data? All Police Forces in England & Wales submit periodic returns to the Home Office that include data on their uses of forensic bioinformation. The purpose of these returns is largely to monitor the performance of Scientific Supports Units, and this purpose shapes decisions about what information to collect from whom, and how it should be analysed, reported and used. These same data may also be examined within forces in order to compare the performance of different units (and sometimes different individuals) within their own organisation. The focus of all of these national and local efforts has been to standardise data for meaningful inter and intra-force comparisons, at least as far as the uses of bioinformation to support the investigation of volume crime is concerned.
- 3.25. However, even when such periodic returns are accurately recorded, they do not necessarily allow an adequate estimation of the quality and quantity of the contribution of forensic bioinformation to criminal investigations and detections. Partly this is because not all instances of the collection of forensic bioinformation are recorded. For instance, if a non-police officer recovers biological material (i.e. a pathologist/ forensic medical examiner) then this will not be recorded in the force periodic returns. There may also be many instances in which the failure to match a DNA profile or identify a fingerprint to a particular suspect may appear to be a negative result, but such negative results may play an important part in excluding particular individuals from further investigative inquiries and/or by giving further direction to an investigation.
- 3.26. Individual forces may also supplement the data required by national agencies with their own data, for example by recording the temporal order in which particular forensic results were obtained, the time taken to achieve them, and the time taken to act on them. But these more detailed efforts normally follow the use of bioinformation only to the point of 'detection' in the criminal process, and even here there can be difficulty in assessing the manner in which the availability of bioinformation assisted the achievement of a detection. This is especially true in the case of serious crime investigation, but is also the case in

⁹⁵ NPIA website, accessed 1st December 2009.

routine volume crime investigations where administrative systems do not necessarily permit nuanced recording of the forensic contributions to the investigative process.

- 3.27. Prior to the introduction of The Scientific Work Improvement Modelling Programme (SWIM), the Police Standards Unit (PSU) utilised a simple linear model in which it was assumed that simply attending more scenes to collect additional forensic material would result more detections. SWIM was developed in response to concerns that where there were backlogs in processing or acting on bioinformation and other forensic intelligence, greater scene attendance would only add to the backlogs. Greater attendance would not necessarily improve detections or to the degree suggested by some commentators. The assiduous collection of fingerprints and biological samples from scenes of crime has to be matched by the adoption of equally rigorous and efficient processes all the way through the CJS. Any analysis of the effective uses of bioinformation based on police force returns will have to be able to map the changes in significance of forensic bioinformation as progress is made through successive stages of the criminal process.
- 3.28. An alternative source of data - The Police National Computer (PNC) was not designed to facilitate the collection of data relevant to questions about the effective uses of forensic bioinformation, or deliver large 'chunks' of data. The PNC data are limited largely to demographic/ operational and conviction data.

Forensic Bioinformation: Bespoke Research Studies

- 3.29. If the analysis of police force returns currently does not provide a sound basis for assessing the effective uses of forensic bioinformation, it is disappointing to note the seeming absence of an accumulating body of knowledge derived from existing research studies in this field. In the UK, research has been mostly undertaken/ funded by the Home Office and disseminated through Home Office channels. Whilst some studies, like 'Pathfinder' have sought to track individual cases through the criminal justice process, this process has proved to be difficult and time consuming. Other Home Office funded studies have sought to throw light on the police uses of forensic bioinformation, but it seems that enthusiasm for commissioning such studies by independent researchers has waned over the last few years. There is insufficient space to provide details of all of these studies, but readers interested in their details can consult a systematic review of findings relating to volume crime investigations published by the Home Office in 2005.⁹⁶ Additional analysis of, and arguments

⁹⁶ Bradbury, S-A. & Feist, A. (2005) *The Use of Forensic Science in Volume Crime Investigations: A Review of the Research Literature*. London: The Home Office.

concerning, such studies can be found elsewhere.⁹⁷ While all suggest that the role played by forensic bioinformation in detecting crime is significant, the detailed trajectories of its uses – its successes and failures - remain poorly articulated. Additional uncertainties exist about the uses of forensic bioinformation in serious crime investigations. There is hardly any published research that focuses on these kinds of cases, and this is especially difficult to understand given the Government's reiteration of claims for the importance of DNA databasing for the detection of murders and rapes.

- 3.30. In the absence of independent peer-reviewed research on the use of forensic bioinformation it is difficult to know the extent and quality of the knowledge base on which police and other criminal justice actors base operational and policy decisions in this domain. Whilst NPIA Guides and ACPO and other Manuals may seek to represent the 'best' utilisation of forensic bioinformation, such prescriptive accounts may depart from actual practice in many cases. Manuals are not a substitute for empirical research on this topic. There is little collaboration between the police and external researchers, and internal reports and documents are not widely circulated outside of operational circles.
- 3.31. Whilst it may be difficult to undertake research in this field (especially in the investigation of serious crime) there is scope for doing so if all parties to such work understand its potential benefits. However, it would be important that such work was not overwhelmed by the immediacy of political preferences and instead was able to develop through a joint commitment to the production of high quality evidence relevant to the operational uses of bioinformation.
- 3.32. It will also be very useful to compare the situation in England and Wales with policing research elsewhere in the world. There may be better integration of academic research in other European jurisdictions, although this assumption needs to be tested. The situation in North America is also unclear, although NIJ funding has been used to facilitate some research on the uses of forensic science to support criminal investigations. The recent NAS Report may encourage the further development of academic/police partnerships.
- 3.33. Two recent US studies provide a sense of what might be possible given appropriate levels of funding and the development of such partnerships in England & Wales. Both are ambitious pieces of work, the first being the only known instance of the use of an experimental design to determine the effects of the use of DNA profiling on volume crime investigations, the second being a wider survey of the use of a larger range of forensic technologies, including

⁹⁷ For example, Williams, R. and Johnson, P. (2007) Trace Biometrics and Criminal Investigations, in Newburn, T., Williamson, T. and Wright, A. (eds.) *Handbook of Criminal Investigation*. Cullompton: Willan, pp. 357-80., and in Williams, R. (2008) Policing and Forensic Science, in Newburn, T. (ed.) *Handbook of Policing* (2nd Ed). Cullompton: Willan, pp. 760-93.

forensic bioinformation.⁹⁸ It remains to be seen whether there is the political will to encourage and fund such studies here.

- 3.34. In the US, lessons are being learnt from DNA exonerations. It may be that a similar de-construction of miscarriages of justice in England and Wales may be useful and map where mistakes occur in the criminal process. Study of exonerations in the US,⁹⁹ have exposed the limitations of techniques such as serology and bite marks, and also how scientific testimony might not be credible or be distorted in cross-examination or when a case is summed-up. This is something within the remit of the CCRC but their only attempt to conduct such research was a study of 80 initial referrals within which sample there were said to be 26 examples of flawed or problematic forensic science. The absence of a database of such cases that could be interrogated has been an obstacle to systematically following-up concerns about expert evidence exposed by cases such as the *Cannings* appeal. The Omagh trial was seen to be a clear example where significant errors had been made during the trial – not just in respect of the actions of police officers - but also in understanding the scientific issues within the court room.
- 3.35. The communication of forensic evidence in court is crucial and yet remains under-researched. The significant issues of how forensic bioinformation is used/ portrayed/ dealt with during trials are highly complex. Consideration of these issues has in turn raised questions about the ability of the adversarial system to cope properly with expert evidence. The Law Commission have recently examined this area and proposed reforms to the reception of expert evidence, although their deliberations were incomplete at the time of writing.¹⁰⁰

Cost-effectiveness and Forensic Science Utility

- 3.36. The interest in the criminal justice system consumption of GDP has been manifest from the mid-nineties onwards. While there has been a recent retreat from the use of a battery of performance indicators (PI) in policing, demands for the evaluation of cost-effectiveness are likely to intensify as the recession intensifies fiscal constraints. With the highest level of CJS expenditure in G8 countries when measured as a proportion of GDP, UK police forces and forensic providers can expect increasing scrutiny from budget managers and their accountants.

⁹⁸ The first of these studies has been published (see Roman, J.K. *et al* (2008) *The DNA Field Experiment: Cost Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes*. Washington: Urban Institute. The second, carried out by Peterson and colleagues at the University of California is currently under review and awaits publication.

⁹⁹ Garrett, B.L. and Neufeld P.J. (2009) 'Invalid Forensic Science Testimony and Wrongful Convictions' *Virginia Law Review*, 95:1-97

¹⁰⁰ Law Commission of England and Wales (2009) *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales: A New Approach to the Determination of Evidentiary Reliability*. Consultation Paper no.190. London.

3.37. One of the major obstacles to cost evaluation in policing identified at the beginning of this project is the problem of measuring inputs. Initially this arose because of the difficulties in measuring police expenditure on different activities. In recent years ACPO had effectively created a competitive market for many forensic science services. At first sight this should result in better input information. It was suggested by some participants in the seminars however, that one of the results of the procurement exercise had been to create a false sense of the cost of forensic provision, with inadequate account by procurement managers of the ability of smaller providers to guarantee timely delivery and quality of results. The procurement exercise may have led some to believe that 'value for money' was synonymous with 'lowest price'. Also, while the cost of DNA use could be measured (albeit imperfectly) from such prices, it is unlikely that the cost of fingerprint work could be made available on an approximately comparable basis.

3.38. The two key measures that have been proposed for assessing value for money in policing are 'cost-effective analysis' (CEA) and 'cost-benefit analyses' (CBA). The former is used to compare input costs. The latter is more complex. Having valued all inputs, outputs and outcomes in monetary terms, it compares competing options for spending money to identify the highest achievable net benefit. Further complications arise when there is inconsistency in calculations regarding the inclusion of staff costs as well as laboratory costs for example. More recently ONS (The Office of National Statistics) has been seeking to develop a methodology to measure CJS productivity. This is defined as 'a ratio of CJS outputs to CJS inputs at constant prices'. This approach appears to have been based on CBA; it places a greater emphasis on the importance of outcomes compared with outputs. The ONS paper on this subject contains two caveats about their proposed approach:

- It may be unclear which observed or recorded changes can be attributed directly as outcomes to improved CJS productivity or result from other factors (e.g. is a reduction in the theft of or from vehicles the result of improved CJS detections achieving the detention of offenders or, alternatively, better security by manufacturers and owners)?
- In contrast to the ONS approach, the Administration of Justice (AoJ) methodology that the Home Office began to develop earlier recognises the interdependence of CJS agencies, for example, improved detection of offenders by the police may be negated by the absence of effective follow-up by the CPS, courts and NOMS (National Offender Management Service).

3.39. The ONS have also acknowledged that some outcomes have a greater value or address more serious concerns than others, for instance, car crime is generally more tolerable than burglary. During seminar discussion, further limitations in

the ability to measure value for money or the reliability of the results of such work were identified:

- The sometimes dispersed (temporally and geographically) benefits from acquiring bioinformation, for example, cold case reviews might result in the detection of crimes by using forensic information collected and then stored for several decades, and international cooperation might result in criminals being identified from databases created and maintained by other states.
- Unanticipated benefits including the utilisation of investigation capabilities for DVI purposes (e.g. the international response to the 2004 Tsunami).
- Evaluation methodologies may also need to qualify reduced input values by making an adjustment for any consequential loss of output in terms of research and development investment where the ability to engage in R&D is curtailed by procurement strategies or decisions based solely on price.

3.40. There are many precedents in other areas of econometrics where research combines objective and subjective measures and seek to evaluate short-term and long-term impacts. Consideration should be given to weighting outcomes by something equivalent to cost-utility analysis in health economics (e.g. 'quality adjusted life year' that reduces inherent discrimination in CBA against people with a lower earning capability). There have also been attempts to formulate a multi-attribute decision-analysis in energy/ environment and health arenas to try and elicit value-based weightings in decisions.

3.41. The most promising area for evaluating what can be achieved through forensic science might be major crimes. Case reviews provide an opportunity to obtain data from case support and scientific support units. With the analysis of a sufficient number of cases it might be possible to robustly estimate the cost-benefits of forensic science inputs. Although the full range of inputs/outputs might be overlooked, miscounted or unquantifiable (e.g. a scene of crime visit that did not yield trace bioinformation but resulted in crime prevention advice being acted on).

3.42. There are always going to be different levels of 'value' in such evaluations. There may always be a cash value for the decisions facilitated by particular types of forensic evidence. There will also be intangible/ (intrinsic) 'values' in terms of the ability to successfully detect crimes (community values) and these may be harder to capture and measure. Research may be undertaken but may require caveats because of the complexity of the social and legal dimensions that may affect interpretation. Moreover, many pilot studies or focused work produced results that reflected a level of resource that was not available when working normally and such results were unlikely to be replicated in national trends. Also much research does not answer the questions that we are now

asking. Attrition studies are intended to identify where cases fell out of the system not crime reduction or displacement, and for all forms of investigation not just forensic science. We are now trying to fit bits of research into a very different agenda and asking questions of earlier research that it cannot answer.

- 3.43. One difficulty with evaluations is the lack of stability within the criminal justice policy-making arena – very often politicians are short-termist, and decisions to change priorities and redeploy resources may be presented in order to give the impression that additional resources have been provided for CJS purposes. Independent experts can build better models and can make evaluations about long-term values/strategic objectives for the criminal justice system etc. (one example that longer-term CJS transformation is possible was the abolition of capital punishment against the opposition of large segments of the press and the instincts of some senior politicians).
- 3.44. Other problems in evaluation arose when benefits take time to be realised or are dispersed. The Dutch were able to demonstrate back in 2004 that without necessarily achieving immediate detections, they could build up via their DNA database patterns (by offence and location) of collaboration between different criminals that might later prove to be significant later in the light of new (possibly quite different) information. The Belgian database has been used to demonstrate that DNA could link serious offences committed in that country, the Netherlands, Germany and France. The inputs and outputs for this activity, however, would be scattered over four jurisdictions.
- 3.45. In considering the three issues of data sources, research, and value for money evaluation, participants in seminars often made comparisons between the medical and criminal justice domains, particularly the role in the former played by the UK National Institute for Clinical Excellence (NICE) which enjoys significant technical, scientific and professional independence from Government as well as from professional and commercial interests. During seminar discussions there was some support for considering the possibility of learning from this health model.
- 3.46. The 'ultimate issue' for most of those contributing to seminars was the question of what value forensic bioinformation can be shown to add to the criminal process/ criminal justice system. It may be necessary to consider different methods of data collection to give more information on different 'outputs'. This would depend on what the 'outputs' were considered to be and how they may be measured. It may not be complex to create new measures and collate data but would require substantial resources. It may also require significant human intervention (which is costly) because the type of data required would necessitate judgments of relevance to criminal justice processes. Any 'rich' data

collection would also require the support of other agencies – in particular the CPS (Crown Prosecution Service). However, the CPS previously have expressed no interest in collection/ returning data for these kinds of research purposes.

Conclusion

3.47. There is wide agreement of the necessity to strengthen the current evidence base for the use of forensic bioinformation in support of criminal investigations and prosecutions. This can be seen in Government statements, in the work of advisory bodies and in the reports of Parliamentary Committees. It was also a theme throughout many of the discussions held in the course of this project. We endorse the view of the Human Genetics Commission that "...the compiling of an evidence base that would demonstrate the utility of the NDNAD as an investigative and probative resource is, we believe, an urgent and important task."¹⁰¹

3.48. The Human Genetic Commission's recent report '*Nothing to Hide, Nothing to Fear*', includes an important section dealing with the issue of research and evidence on the uses of forensic bioinformation. In this section, entitled 'Forensic Utility', the Commission lay out a strong case for the necessary development of a programme of research, recommending that

"...data supporting evaluation of the forensic utility of the National DNA Database should be collected and published by the National DNA Database Strategy Board or the National Policing Improvement Agency National DNA Database Delivery Unit. An evaluation of such data should be conducted by an independent body and placed in the public domain."¹⁰²

3.49. The provision of enhanced NDNAD information should clearly be an element in any programme of research, although in several of our seminars, participants pointed out that these kinds of suggestions for the provision of 'better data' place immense demands on existing information management systems, and indeed sometimes could only be met by the introduction of new and expensive supplements to them. Intensive work would need to be done to identify the kinds of questions that could be asked about 'utility' as well as the kinds of data that might permit them to be answered. This work would itself necessitate discussions between a number of academic, operational and policy actors.

¹⁰¹ Human Genetics Commission, *Response to "Keeping the Right People on the DNA Database"* August 2009, para. 22.

¹⁰² HGC '*Nothing to Hide, Nothing to Fear*' (Department of Health, London, 2009) p.70.

- 3.50. In addition to the issue of IT support for the provision of standardised information, a strong case can be made that a wider range of studies should be commissioned and supported by key agencies, including relevant funding bodies, forensic providers, police users, and the Home Office. Such an enhanced forensic bioinformation research programme will need to take into account other forms of bioinformation. It seems obvious that the uses of IDENT1 should be considered alongside the collection of information about the NDNAD. However, there are also good reasons for extending the reach of research beyond a consideration of databases as such in order better to understand the very wide range of uses of forensic bioinformation that occur in the course of criminal investigations. Many of these uses may be highly significant in supporting investigations but are not well captured by counting DNA matches between scenes and subjects, or the successful identification of fingermarks. Some highly significant uses of DNA profiling and fingerprint technology may not use relevant databases at all, and even when they do, it is not necessarily a matter of using them to identify an unknown offender but for a series of other purposes of relevance to a particular investigation.¹⁰³
- 3.51. Other countries, especially the USA, seem to have begun the establishment of such a programme more easily than the United Kingdom, although such work is at a seemingly early stage and is in danger of dominated by a preference for one particular methodology – randomised control trials.¹⁰⁴ In the absence of a UK body equivalent to the NIJ in the US, and in the light of probable budgetary constraint, any call for enhanced funding for a wider range of studies on the uses of forensic bioinformation may seem a tall order, but it is difficult to see how the public debate on this topic called for by Prime Minister Brown in a recent Parliamentary answer can be properly conducted in the absence of such a background.

¹⁰³ These are very varied, but may include for example, helping to determine which of a series of suspects handled any object of interest, inferring what courses of action and patterns of movement have occurred within a crime scene, or which of a series of known persons may have driven a relevant vehicle. It is also possible to imagine other research which utilises such databases for studies related to the detection and reduction of crime in general but which do not directly focus on the investigation of individual cases.

¹⁰⁴ The very interesting response of Ruth McNally to the HGC consultation exercise which informed the preparation of *Nothing to Hide, Nothing to Fear* resonates with some of ideas about the necessity for a wider range of studies. See <http://www.hgc.gov.uk/Client/document.asp?DocId=227&CAtegorYId=4> accessed 12 January 2010.

4 Internationalisation and Exchange

Introduction

- 4.1. This chapter is concerned with the theme of international exchange: both the exchange of information and ideas. While both the previous report of the Nuffield Council on Bioethics and that of the Human Genetics Commission touched upon the international exchange of bioinformation, the paucity of data about such cooperation has restricted the consideration that international exchange has received, despite its relevance to important arguments about sample retention.¹⁰⁵ Convening a series of UK seminars and an international symposium created the opportunity to address this problem by bringing together criminal justice and scientific experts from a range of countries.
- 4.2. The seminars reviewed international biometric exchange arrangements in terms of validity of purpose, technical obstacles, effectiveness and ethical considerations. These elucidated concerns about the foreseeable technological obsolescence of the SGM+ multiplex and the operation of the Prüm Treaty. Seminar participants also had the privilege of hearing views on international co-operation from a father whose daughter's murderer was identified through the international exchange of DNA.
- 4.3. From the first seminar it was apparent that there was a need to address the second quite different aspect of this subject: the exchange of ideas (or in some instances resistance or 'seduction'¹⁰⁶ by outside influences) and increasing internationalisation of decision making and technological development. The *Marper* judgment and the EU Council recommendation that has resulted in the foreseeable technological obsolescence of the SGM+ multiplex,¹⁰⁷ are the principal decisions of this kind for the purposes of this study. It also became clear that some cross-jurisdictional comparisons are made without an attempt to understand contextual variations. Discussion during several meetings reverted to the European Court's attempts to discern the margin of appreciation, particularly through its references to Scots Law. Equally important for many participants was the cautionary note in the *Marper* judgment for countries at the forefront of technological innovation:

¹⁰⁵ Human Genetics Commission, (2009) *'Nothing to Hide, Nothing to Fear'* London, Department of Health; especially pp.70-71.

¹⁰⁶ Dahl, J.Y. and Sætnan, A.R. (2009), ' "It all happened so slowly" – On controlling function creep in forensic science DNA databases', *International Journal of Law, Crime and Justice* (2009), doi: 10.1016/j.ijcj.2009.04.002, where the authors provide an account of the influence or, as they see it, 'seduction' of UK DNA database developments on Norway.

¹⁰⁷ 2009/C 296/01: See para. 4.74.

‘...any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance between the use of modern scientific techniques in the criminal-justice system and important private-life interests.’¹⁰⁸

Beyond these obvious promptings however, there was some acknowledgement among UK participants that technological development had outstripped other considerations.

- 4.4. What emerged from the seminar was consistent with a key insight in the recent Human Genetics Commission report, which noted that technological development could make traditional police databases only a small part of a much wider system – ranging from genetic research to passport databases - containing intimate personal data available to investigators. This could possibly change public attitudes to the forensic use of genetic collections established for quite different purposes.¹⁰⁹ This prompts an immediate question: whether a debate hitherto framed almost exclusively in terms of the forfeiture of privacy in respect of forensic bioinformation might become irrelevant unless it also takes account of the consensual or, perhaps more accurately, quasi-consensual surrender of genetic privacy outside the criminal justice sphere? It has been recently found that people may not be uniformly happy to hand over their DNA for alleged ‘health benefits’ (note the apparent disinterest in available genetic testing kits). There was also great opposition to the sharing of data included in the original Coroners and Justice Bill 2009, and controversy over the testing and storage of babies’ blood spots without consent in the US and Ireland.¹¹⁰

‘Dissolving boundaries’ and ‘Securing the UK Border’

- 4.5. The Human Genetics Commission have noted the growing pressures for sharing information:

‘... there are ... substantial pressures to create the conditions for the horizontal integration of criminal justice databases, and the sharing of information between national jurisdictions. Whereas the exercise of law enforcement powers of European Union (EU) member states are confined within national borders, for the transfer of information relevant to law enforcement these borders are increasingly dissolving. We identify three developments in the ‘third pillar’ of EU policy (police and judicial co-operation in criminal matters) that have contributed to the cross-border linking of forensic bioinformation: the establishment of a system of co-operation based on a central information system making use of electronic databases; the creation of a presumption and then an obligation in favour

¹⁰⁸ *S & Marper v the United Kingdom*, para.111 and 112

¹⁰⁹ *op.cit.* n.105 especially pp.79-80, 83, and 86-87

¹¹⁰ see www.genewatch.org.uk for further details.

of data sharing; and the commitment of the UK and other member states to align with such a system'.¹¹¹

The 'dissolving boundaries' paradigm has been reflected in numerous government statements. These express anxiety about the increasing seriousness and scale of transnational crime and indicate intent to counter it by improving the machinery of cooperation.

- 4.6. Much of the evidence given to the House of Lords EU Committee by the Home Office is informed by this paradigm. The Government explained how the Prüm Treaty would 'speed up and improve the quality and quantity of information exchanged' about DNA, fingerprints and vehicle registration in order to identify and bring to justice terrorists and criminals. Ministers informed Parliament that the Government had negotiated hard 'to get an outcome that enables [them] to sign up to Prüm and get all the benefits in terms of fighting cross-border crime and counter terrorism where so much depends on good data exchange and intelligence led policing'.¹¹² In turn, parliamentarians and ethicists emphasised that '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'.¹¹³
- 4.7. There is also a paradox: that initiatives to harden rather than dissolve national borders may prove to be more significant harbingers of the potential future trajectory for the forensic use of bioinformation than the activities touched upon in the *Marper* judgment. If so, this has major implications for the discourse of rights and privacy. The ethical and legal debate about forensic bioinformation has been conducted largely with reference to collections of genetic material and information gathered as a result of forfeiture. It may also need to take account of what is happening as a result of parallel collections created with the consent or quasi-consent of citizens.

International Cooperation

- 4.8. A study published by the University of Leiden and the Netherlands Forensic Institute in 2000 reported that there was little systematically compiled or published information about international cooperation.¹¹⁴ Half a decade later the situation had not changed, but what could be gleaned did not indicate that a large amount was being exchanged. A report on the sharing of DNA

¹¹¹ *op.cit.* n.105 p.84.

¹¹² House of Lords European Union Committee (2007)18th Report HL Paper 90, Session 2006-07 (London, TSO), Ev.1-2 and Q8.

¹¹³ Nuffield Council on Bioethics (2007), *The Forensic use of Bioinformation: Ethical Issues*, p.105.

¹¹⁴ Joubert, C. and Bevers, H. 'International Exchange of Police Data and Forensic Expertise' in Nijboer, J.F. and Sprangers, W.J.J. M. (eds), *Harmonisation in Forensic Expertise: An inquiry into the desirability of and opportunities for international standards*, Amsterdam: Thelma Thesis 2000, p.485).

information by a DNA Expert Working Group of the European Network of Forensic Science Institutes (ENFSI) reported:

'During 2004 – 2005, the UK received only 149 DNA search requests. These generated 21 potential matches although the majority of the profiles were unreliable; this was due to poor discriminating power. The USA had a similar experience – they received even fewer requests for assistance even though they have a larger database with over 4 million profiles.'¹¹⁵

- 4.9. The reasons for this, in the opinion of the ENSFI experts, reflected inadequacies in current international law enforcement arrangements as well as different technical processes for deriving a DNA profile:

'DNA has proved to be a useful method of identifying criminals and bringing them to justice. However, there has been slow progress in exchanging DNA information routinely between countries. There are various reasons for the slow progress including the differences in Member States' domestic law and data protection arrangements together with the technical complexities around DNA analysis and exchange... Although there have been many successful developments and initiatives to help Member States co-operate to exchange DNA information, the current arrangements are inadequate in their present form. They are incapable of development on a scale that will meet future requirements and they are not always sufficiently transparent or capable of being audited.'¹¹⁶

- 4.10. Summary statistics about the volume of international cooperation initially appeared and have since ceased to be published in NDNAD annual reports. (Compare, for instance, the reports for 2004-2005 and 2005-06 where there are entries dealing with the International DNA Database and, in the former, statistics for international search requests, with the absence of such information in the reports for 2006-2007 onwards.) Last year the authors of another ENSFI report referred to the present 'occasional exchange of DNA profiles between countries'.¹¹⁷ That appears to be an accurate description of the present volume of international forensic cooperation involving DNA.

- 4.11. This could change – within the European Union at least – when the Prüm Treaty takes full effect. The best and most recent indicator of the potential scale of cross-jurisdictional cooperation was revealed in January 2007. The Prüm

¹¹⁵ DNA Expert Working Group of the European Network of Forensic Science Institutes (ENFSI) (2007) Search Request Network Study: Final Report (accessed on 15 April 2007) from the previous ENSFI website: www.enfsi.org/ewg/dnawg/documents/Annex20F20AGISFinal20Report .

¹¹⁶ *supra* pp 5, & 2 (accessed on 15 April 2007).

¹¹⁷ ENSFI (2009) DNA-Database Management Review and recommendations at http://www.enfsi.eu/get_doc.php?uid=345, accessed 06.03.10. p.8.

Treaty had been in force for the purpose of trials of the new arrangements between Germany and Austria for less than two months, but:

'...the automatic information exchange has brought about noticeable operational success: for instance, the German authorities matched DNA profiles of open cases against data held by the Austrian authorities and found hits in 1,510 cases. In this context 710 open traces from Germany could be attributed to persons known to the Austrian criminal prosecution authorities. Broken down by types of crime, 41 hits in homicide or murder cases, 885 hits in theft cases, 85 hits in robbery or extortion cases were found....'¹¹⁸

- 4.12. Both advocates and critics of the Treaty recognise that these results would not necessarily be repeated in the future. There would have been a large amount of information about earlier serious crimes that was available for the first time to the prosecuting authorities as a result of the Treaty coming into force.¹¹⁹ Nevertheless, this was a huge increase in the volume of cooperation involving DNA. The potential of the Prüm Treaty for obtaining serious crime leads more systematically and efficiently could prove to be as significant a breakthrough, for progress in dealing with previously undetectable crimes, as the introduction in England and Wales of cold case reviews of unsolved murders and rapes, or the reversal of miscarriages of justice in the USA.
- 4.13. The installation of the most recent Interpol AFIS system illustrates both how the potential volume of cooperation can increase with improved automation and suggests that this is not always fully exploited. The new AFIS system allows 1000 search requests to be carried out daily, compared with 160 previously.¹²⁰ However, the database is reported to consist of some 100,000 ten prints and 3,000 latent prints, and the number of identifications made during 2009 was in the order of 1,000.¹²¹ Despite initial appearances this appears to be a significant level of cooperation for the exchange of fingerprints. Operating on a sub-continental scale, but within a single unitary state it was reported in 2006 that the FBI IAFIS system had achieved 1,200 identifications with latent prints after it went online in 1999.¹²²

¹¹⁸ House of Lords European Union Committee, 18th Report of Session 2006–07, *Prüm: an effective weapon against terrorism and crime?*, HL paper 90, (London: The Stationery Office Limited) pp. 15-16.

¹¹⁹ *supra* p.16.

¹²⁰ Sagem Sécurité (2009) Press release: Interpol places its trust in Sagem Sécurité once again: <http://www.sagem-securite.com/references-263/criminal-justice-police-264/article/interpol-places-its-trust-in-sagem-securite-once-again>, accessed 090310 .

¹²¹ Interpol Fact Sheet: Fingerprints <http://www.interpol.int/Public/ICPO/FactSheets/FS03.pdf> , accessed 9 March 2010.

¹²² Dror, I.E. and Mnookin, J.L., 'The use of technology in human expert domains: challenges and risks arising from the use of automated fingerprint identification systems in forensic science', *Law, probability and Risk*, Advance Access, published January 22, 2010, p.8. The FBI statistics are likely to reflect jurisdictional responsibilities and like the Interpol data may significantly under represent the scale of cooperation, if much of this is directly between lower level jurisdictions. It does, however, put the Interpol data in context.

- 4.14. The relatively small scale or inherent difficulties of international cooperation involving DNA and fingerprints can also be appreciated by contrasting this data with the detection of criminals travelling with stolen or lost travel documents. At the end of 2008 the Interpol Stolen and Lost Travel Documents (SLTD) database had 16.7 million records and was being used by 145 countries. Several countries are connected directly to the database which can be made interoperable with national border control data systems. In 2008 law enforcement and border control officers carried out 25 million international searches of the database. This resulted in the identification of over 5,000 individuals travelling on fraudulent documents.
- 4.15. Throughout this project, great care was taken to keep the internationalisation of crime in perspective. Most criminals operate locally. Only a small number of successful or dangerous criminals regularly cross borders to evade detection. Investigators present during our deliberations reminded us however, that some criminals who may have recently established themselves as 'local' in the UK will have originated from other countries where records may exist relating to a previous criminal career. Participants with direct knowledge of case cooperation considered that for a minority of crimes (probably many more than the figures above) there need to be systems in place to easily access information from the suspect's home country or countries of passage. This conclusion was reinforced by consideration of a travelling murderer and sex offender who had evaded detection for his most serious offences despite being in custody twice subsequently. When linked to his offences by pure chance, his profile was reanalysed in the USA (because of the use of different multiplex), to be compared with DNA recovered from the crime scene in France.
- 4.16. Our discussions about international cooperation sought to identify the circumstances that might merit the exchange of forensic bioinformation. Under the Prüm Treaty, there is no restriction by offence before a DNA exchange can take place: every crime or arrest could in theory result in a search of all EU biometric databases. In practice, there appears to be growing recognition that a more structured and prioritised approach is needed. Policies developed to prioritise or otherwise restrict cooperation will only apply to anonymous profile comparisons. The results of such exchanges will be provided to the judiciary or the police. They will decide whether to undertake further enquiries. The cost of investigation and the severity of the crime (and perhaps whether the suspect is already in prison) are then likely to determine whether the anonymous match should be followed up.
- 4.17. Within the UK such decisions are not determined, as in Germany, by the law of criminal procedure or, alternatively, subject to judicial or procuratorial supervision as in the Dutch model. Investigators and analysts have the discretion to seek potentially useful information or intelligence. Participants

stressed that not limiting cooperation to specified offences is more likely to assist the investigation of serious crimes. Moreover, when a foreign national is in custody suspected of a crime, it may be in the interests of justice to check whether forensic bioinformation links this person to crimes abroad at the same time as IDENT1 and the NDNAD are searched. Sometimes international cooperation is useful only because organised transnational criminals might lower their guard in their home country. The self-styled 'Pink Panther Gang' was cited as an example of this. The gang had undertaken a series of highly skilled armed robberies in UK, Belgium, France, Switzerland, Dubai and Tokyo, but were difficult to detect as members withdrew to their safe havens in Serbia and Croatia. However, some gang members committed minor offences in their home countries and because the local police shared their information through Interpol it was possible to arrest thirty or so members of the gang.

- 4.18. Limiting international cooperation to serious or organised crime may result in failures to identify such successful criminals or their activities. For example, a series of thefts from lorries in Belgium and the South Netherlands were considered minor property crimes. Over time however, analysis revealed a pattern of events of much greater significance. Indeed some investigators consider that the most effective way of solving serious crimes is for the police to allocate adequate time and resources to investigating volume crimes. Those responsible for serious (and often sexual) offences will normally have a background of burglaries or property crimes. Sometimes they might deliberately commit minor crimes in one country to obtain money, and serious crimes, including serious sexual assaults in another.
- 4.19. This does not necessarily mean, irrespective of available resources, that all crimes should be investigated or that all requests to cooperate with an investigation should be accepted. An initiative to categorise the comparative nature of criminal offences, in terms of the substantial offence would be an appropriate early step in developing an international framework that might give greater coherence to international cooperation, rather than by simply trading caps in the volume of cooperation that each country will agree to process. For example, many countries may be confused by the nature of UK terrorist and national security related requests. Murder or homicide is a serious offence, irrespective of known or suspected terrorist involvement or motivation, but the effect of some of the recent declaratory 'terrorist' offences may have been to misleadingly brand individuals guilty of trivial transgressions or, in the case of protests associated with the invasion of Iraq, those who expressed dissent from what is seen by many authorities on international law as unlawful action by the Government, as threats to international security.

Bioinformation outside the criminal justice system

- 4.20. A project visit to China, including the Hong Kong SAR (Special Administrative Region), caused us to reconsider our earlier lack of engagement with the use of bioinformation outside the traditional criminal justice sphere. There DNA is seen as much more important for border control than criminal justice purposes. Since 1980, immigration from the Chinese mainland to Hong Kong has been subject to a strict quota. The number was originally limited to 75 per day. It was gradually increased to 105 in 1994, and then to the current quota of 150 in 1995. Most of these migrants are allowed to enter Hong Kong in order to be reunited with their families.¹²³ Entitlement to entry under this scheme is established through DNA testing.¹²⁴ During 2007, 34,000 (on average 93 each day) mainlanders joined their families in Hong Kong under the One-way Permit Scheme.¹²⁵ In contrast the annual number of arrests in Hong Kong analysed quinquennially between 1990 and 2005, ranged between 41,000 and a peak in 1995 of 53,000.¹²⁶ The use of DNA subject profiles for border or migration control purposes, given that bioinformation is likely to be relevant to the minority of offences, will be more frequent than for criminal investigations.
- 4.21. Great Britain is significantly different to Hong Kong in terms of the levels of controlled immigration from outside the free movement area of the EEA plus Switzerland and recorded crime: proportionately (i.e. per 100,000 residents), 40% lower and four and half times greater.¹²⁷ However, biometric collections of data for border and migration control purposes are likely to become as significant in the UK in future years, as they are in Hong Kong.
- 4.22. During the current forensic biometrics debates and inquiries, little attention has been paid to the evolution of UK border control policies and practice. Several recent developments – bundled together in a 2007 Home Office document entitled 'Securing the UK Border'¹²⁸ – and subsumed subsequently within the UKBA's e-Borders programme, need to come within the mainstream of forensic

¹²³ Asia Pacific Migration Research Network (APMRN) (undated) Migration Issues in the Asia Pacific: Issues Paper From Hong Kong <http://www.unesco.org/most/apmrnw7.htm>, accessed 1 February 2010.

¹²⁴ Project members' discussions at government laboratories in Hong Kong and Beijing on, respectively, 9 and 13 November 2009.

¹²⁵ Government of Hong Kong (2007), Yearbook for 2007, page 406 <http://www.yearbook.gov.hk/2007/en/pdf/E20.pdf>, accessed 1 February 2010.

¹²⁶ Broadhurst, R., King, W.L. and Ching, LC (2008), 'Crime trends', p.62 in (eds.) Chui, W.H. and Lo, W.L., *Understanding Criminal Justice in Hong Kong*, Cullompton, Willan.

¹²⁷ The UK and Hong Kong data appear to be, respectively, in the order of (controlled immigration) 287 in twelve months ending 30 September 2009: 490 in 2007 and (arrests: note England and Wales only) some 2,700 in 2008: 590 in 2005. This is based on UK data for the number of persons (excluding EEA and Swiss nationals) granted settlement during the 12 months ending 30 September 2009: 176,270 (Home Office (2009) Control of Immigration Quarterly Statistical Summary, United Kingdom: July – September 2009, <http://www.homeoffice.gov.uk/rds/pdfs09/immig309.pdf> Home Office (2009) and (at the time of writing) the latest data for arrests in England and Wales: 1,475,000 in 2008 (Ministry of Justice 2010) Criminal Statistics: England and Wales 2008 <http://www.justice.gov.uk/publications/docs/criminal-stats-2008.pdf>, p.16 and both accessed 1 February 2010.

¹²⁸ Announced in a Home Office Press Notice dated 28.03.07: Government To Strengthen "Off-Shore" Border, <http://press.homeoffice.gov.uk/press-releases/off-shore-border.html>, accessed 2 February 2010.

biometric scrutiny. Two of these will result in database retention and the incorporation of a standard set of Home Office biometric data within an identity or travel document. This data will consist of a set of ten prints and digital facial image theoretically capable later of being used within automated facial recognition systems. Enrolment within this parallel system will be as follows:

- A compulsory identity card for foreign nationals (ICFNs) was introduced in November 2008 for migrants from outside the European Economic Area (EEA) and Switzerland. The card is being introduced gradually and is currently issued to a wide range of migrants and their dependants when they apply to extend their stay in the UK and will also be used for checking identity at border crossings.¹²⁹
- In addition to checking the biometric data in ICFNs, from 30 November 2009, fingerprint checks were introduced at the UK border for all passengers required to use biometric UK visas and entry clearance documentation.¹³⁰ As a result every visitor with a nationality to which visa requirements apply are now checked against watchlists to identify failed asylum seekers or anyone who has previously been removed from the country.¹³¹

4.23. UK citizens and foreign nationals with residency or entry rights have been encouraged to enrol in a fast-track border control system named IRIS. Between September 2008 and the 2006 launch of this voluntary iris scanning programme, 217,000 people had enrolled. However, this scheme may not be extended beyond the original four airports. In addition to technical failures and difficulties in providing access for enrolment, there are doubts about whether iris scans can cope with high volume usage. UKBA are reported to be looking at other biometric options such as facial recognition and fingerprints, possibly 'privately funded rather than funded by the UK government'.¹³²

4.24. Migration statistics are complex, based on inadequate data collection designed originally for other purposes and subject to significant methodological debate. As a result they have been described by the Statistics Commission as 'weak'.¹³³ However, data published by the House of Lords Economic Affairs Committee suggests that up to approximately 5.5 million immigrants (some 9% of the UK resident population) originated from outside the EEA travel zone. Most will be

¹²⁹ UKBA website information at

<http://www.bia.homeoffice.gov.uk/managingborders/idcardsforforeignnationals/>, accessed 1 February 2010.

¹³⁰ UKBA Press Release 25 November 2009 Introducing fingerprint checks at the border, <http://www.bia.homeoffice.gov.uk/sitecontent/newsarticles/2009/november/introducing-fingerprint-checks>, accessed 1 February 2010.

¹³¹ Airport-technology.com (2008) Body Check: interview with Julie Gillis, of the UK Border Agency, on website, <http://www.airport-technology.com/features/feature41603/>, accessed 2 February 2010.

¹³² *supra*.

¹³³ House of Lords Select Committee on Economic Affairs (2008), *1st Report of Session 2007–08: The Economic Impact of Immigration, Volume I: Report*, p.10 (London: The Stationery Office).

enrolled within in these new biometric collections.¹³⁴ The number of enrolments will be increased by travellers whose citizenship brings them within the scope of the biometric visa scheme. Even conservative estimates suggest this is likely to add an additional two million people annually to border control biometric databases.¹³⁵ This will be dwarfed however, by the standard sets of Home Office biometric data collected with the introduction of biometric passports and identity cards for British citizens. These are issued separately by the Identity and Passport Service to UK citizens. While the number of identity cards issued can be counted (at the time of writing) in thousands, some 5.25 million new passports were issued in 2008-2009.¹³⁶

4.25. The latest reported increase in the number of personal profiles held on NDNAD amounted to some 580,000 in the year up to 31 March 2009, resulting in the retention of data relating to an estimated 4.8 million people (NDNAD Annual Report for 2007-09). Post-*Marper* retention rules will result in a reduction the scale of NDNAD operations and in the volume of data held. Irrespective of the impact of this change, it is inevitable that the size of the criminal justice biometric databases will soon be exceeded by the collections of data biometric collected by the Identity and Passport Service and UK Border Agency. For almost half a decade the Home Office has anticipated running 'a highly reliable biometric enrolment and verification system with 40-50 million people enrolled', although it may not have been able to operate at this scale by 2006, as originally planned.¹³⁷

4.26. Biometric data held by UKBA can be shared with the police, security services, customs and other agencies, possibly private contractors, within the UK and abroad. Such cooperation is governed by the Code of Practice on the management of information shared by the Border and Immigration Agency, Her Majesty's Revenue and Customs and the Police issued in 2008.¹³⁸ This code is clear and comprehensive about the collection of data and the purposes to which it can be used, with requirements for access control, audit, and penalties if information is mishandled or misused. In contrast to MOPI (see para. 5.34), it was brought into force as secondary legislation (Negative Resolution Procedure). Its chief limitation is the fact that it only applies to UKBA, police and Customs staff. The code does not appear to apply to carriers, contractors and security services.

¹³⁴ *ibid.* p.12.

¹³⁵ For details of potential numbers see: Office for National Statistics (2009) *Travel Trends 2008: Data and commentary from the International Passenger Survey* (Newport, Office for National Statistics), Table 2.09, p.33 accessible at http://www.statistics.gov.uk/downloads/theme_transport/Travel_Trends_2008.pdf.

¹³⁶ Identity and Passport Service (2009) *Annual Report and Accounts 2008-09*, HC 629 (London: The Stationery Office), p.4.

¹³⁷ House of Commons Science and Technology Committee (2006) *Identity Card Technologies: Scientific Advice, Risk and Evidence*, Sixth Report of Session 2005-06 (London: The Stationery Office), Ev119.

¹³⁸ Available at: www.bia.homeoffice.gov.uk . accessed 3 April 2010.

4.27. An even greater omission in the governance of non-criminal justice bioinformation is that there do not appear to be any published regulations governing access to or the sharing of biometric information held or collected by the IPS in connection with identity cards and passports. For example, there appears to be no information in the public domain about whether or not, and if so, under what circumstances, fingerprint data held in those later two sets of documents can be speculatively searched against latent prints held on NAFIS or vice versa. The different controls, or absence of controls, over what appear at first sight to be separate collections of data is made worse by the fact that they are held on the same system. Initially at least, a single database holds both the visa biometrics of foreign visitors from outside the EU, and the identity card and passport biometrics of UK citizens. This collection of data is interoperable with the basic demographic, employment and tax related national insurance records of virtually UK citizens held on the DWP's Customer Information System (CIS).¹³⁹

4.28. In devising its standard set of biometric data, the Home Office, in contrast to its pioneering role in DNA, was following a pattern set by other countries, the International Civil Aviation Organisation (ICAO) and the European Union:

- Following 9/11, the United States introduced biometric (fingerprint) visas for visitors;
- In May 2003, ICAO adopted a blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs). This nominated facial recognition as the primary biometric with iris and fingerprint as backup;
- In June 2003, a border control programme based on iris scanning was rolled out throughout the United Arab Emirates;
- In December 2004, following European Parliamentary approval, a new Regulation on passports in the Schengen States was adopted, providing that newly-issued passports must include digital facial images (within 18 months) and fingerprints (within three years).¹⁴⁰

This does not indicate a lack of ambition in the Home Office. A 2006 report by the House of Commons Science and Technology Committee noted that none of the above initiatives were on the same scale or simultaneously encompassed three types of biometrics. As noted however, in connection with the pioneering use of forensic bioinformation, issues of governance sometimes appear to have taken second place to ambitions to provide a technological lead to the world.

¹³⁹ Home office (2008), *National identity Scheme Delivery Plan 2008*, p25 (London: Identity and Passport Service).

¹⁴⁰ *op.cit.* n.136, p. 9 and 11.

- 4.29. The use of DNA for border control purposes, on the Hong Kong and China model has made a relatively late and problematic appearance.¹⁴¹ The initial foray by UKBA into the use of genetic techniques for determining asylum was described in an editorial in *Nature* as 'scientifically flawed, ethically dubious and potentially damaging to science'.¹⁴² In September 2009, UKBA announced the launch of the 'Human Provenance Pilot Project' as a joint project with SOCA and funded by the FCO. It is intended to deal with concerns about possible 'nationality-swapping', and to challenge Home office entry decisions, as in Hong Kong, one element of the pilot is the use of DNA to verify relationships between adults and children. According to information provided by the Home Office to the House of Commons Science and Technology Committee Select Committee this is intended, as one project objective at least, to evaluate the use of DNA to prevent child-trafficking, as within China. The main aim however, appears to evaluate whether DNA analysis and isotope comparison can test country of origin claims. For example, would it enable UKBA to distinguish between a Somali entitled to asylum status and someone from an adjoining East African country who is not?
- 4.30. UKBA indicate an intention to consult the Home Office Forensic Science Regulator about ethical approval and scientific validity:

'At the conclusion of this pilot we will review the results, including the underpinning science and the ethical implications of the work. The Forensic Regulator will also be consulted during the period of the 3 month pilot. Only if the evaluation and regulatory review is positive, will UKBA proceed to use the results of future tests to support the decision making process in specific cases.'¹⁴³

Participation was said to be voluntary. But the first language of participants is unlikely to be English and given their vulnerable nature, informed consent would be difficult to establish. UKBA caseworkers were initially at least, encouraged to 'draw a negative inference as to the applicant's credibility' when making asylum decisions, if the asylum seeker refused to provide samples for the trial. In the face of ethical and scientific concerns the status of the initiative changed, becoming a proof-of-concept project.

- 4.31. The project raised ethical and sociological questions about whether nationality and family relationships are conferred by law, e.g. by official birth registration,

¹⁴¹ For what follows the facts are drawn chiefly from the *Nature* editorial; an analysis by the HGC Secretariat: Human Genetics Commission in (2009), Paper HGC09/P25; and The UK Border Agency's Human Provenance Pilot Project, available at (accessed 02 February 2010)

www.hgc.gov.uk/.../HGC09%20P25%20%20Human%20Provenance%20Pilot%20Project.doc and Brice, P (2009) A PHG Foundation news report dated 30 September 2009: DNA testing to assess nationality of UK asylum seekers, <http://www.phgfoundation.org/news/4855/> accessed 03 February 2010.

¹⁴² 'Genetics without borders', *Nature*, vol. 461, Issue no. 7265.

¹⁴³ The Government Office for Science (undated) from information provided by the Home Office for a House of Commons Science and Technology Select Committee: Evidence Check (accessed 3 February 2010) p12.

or might be established through family practice, or alternatively, must be validated biologically. The scientific methodologies – most of which have been developed for the study of populations not individuals - are equally problematic:

- Little research has been carried out on DNA markers and populations in Africa. As a result comparison databases will be limited and less able to provide an accurate picture of ancestry and certainly not on a local scale;
- Y-chromosome analysis can be thrown off by a distant male ancestor;
- SNP (single nucleotide polymorphisms) -based identifications can be problematic, individuals whose parents come from two geographic regions are often classed into a third region from which neither parent originated;
- The proposed hair and nail isotopic signatures that were to be used can probably only give an indication of place of residency for the past few years;
- The Adam's torso case, which appears to have been presented by UKBA as proof that UKBA proposed to use an "internationally recognised" comparison method was performed by bone analysis. Moreover, the methodology in that case has not been explained in scientific publications or examined in court for the purposes of establishing nationality.

Nature reported that UKBA claimed that the project had undergone peer review, but that the agency did not provide details. Several geneticists contacted by the journal had seen a preliminary proposal in 2007 and warned that it was unlikely to work.

The Significance of Scotland

4.32. Hepple has commented that the *Marper* decision strongly hints 'that uniformity with Scotland would be acceptable as being within 'the margin of appreciation' open to the UK Government'.¹⁴⁴ Comparisons with Scotland were made during the seminars and international symposium. It became increasingly apparent during these discussions that there was little recent research on the use of DNA in the two jurisdictions. In particular we noted an absence of efforts to place the difference in law within the context of how different arrangements emerged, the state of available evidence about the operation of the Scottish system and broader criminological and other factors that are important when making cross-jurisdictional comparisons.

4.33. Williams and Johnson recognised in 2004 that 'the kinds of operational issues that will arise in the future for a number of police forces wishing to share intelligence information across the EU are already visibly prefigured in the current arrangements that exist to make possible the linkage of collections of

¹⁴⁴ Hepple, (2009) 'Forensic databases: implications of the cases of *S* and *Marper*' *Medicine, Science and the Law*, v. 49 no.2 p. 82.

forensic DNA profiles across jurisdictions within the United Kingdom'.¹⁴⁵ Such a comparison remains the only detailed source of information about cross-jurisdictional biometric cooperation. With the passage of time it is possible to provide a greater degree of analysis as a result of the wealth of information, albeit not always consistent, that can be gleaned from NDNAD reports.

The legal position in Scotland

4.34. Under Scots law a subject DNA sample can be taken upon arrest for an imprisonable offence and speculatively searched against both the Scottish DNA database and NDNAD. However, profiles must be destroyed if the individual is not convicted or is granted an absolute discharge. Since the Police, Public Order and Criminal Justice (Scotland) Act 2006, an arrest for certain sexual or violent offences may permit the retention of the sample and profile for three years from the date of arrest, even if the arrestee is not convicted. Upon application by the chief officer to a sheriff, an extension of up to two years may be authorized, where it has been demonstrated that there are reasonable grounds for retention. The Scottish arrangements also anticipated the Crime and Security Act 2010 with regard to volunteer samples. An individual may withdraw consent for the retention of the sample and related profile at any time.

Data sharing between jurisdictions¹⁴⁶

4.35. The scale of personal data sharing and the annual volume of data transactions across the jurisdictional boundary are summarised in Table 4.1.¹⁴⁷ All subject profiles taken in Scotland are uploaded to both the Scottish database and NDNAD. However, a profile from a sample recovered from a Scottish crime scene is only uploaded to the NDNAD if it did not result in a match on the Scottish database.¹⁴⁸ This is an effective and efficient arrangement for administrators and the criminal justice systems on both sides of the border. As such it is a potentially useful model for crime scene profile cooperation within a devolved or federal structure, or internationally. The results obtained from such interoperability are summarised in Table 4.2.¹⁴⁹

¹⁴⁵ Johnson, P. and Williams, R. 'DNA and Crime Investigation: Scotland and the 'UK National DNA Database' *Scottish Journal of Criminal Justice Studies* 10: 71-84.

¹⁴⁶ Note to the tables in this chapter: 1. NDNAD Data has been taken from the relevant NDNAD report but has not been adjusted to reflect the practice by which, from time to time, historical data has been revised in subsequent NDNAD Reports. An example of this is the 'slight difference' in data about the annual uploading of profiles at 31/03/09. Such changes are judged to be less significant than maintaining internal consistency for all figures published in a specified year, not all of which have been subsequently republished in a corrected form in line with other changes in the data. 2. Where the data cannot be read directly in the report this is indicated by the addition of '(est.)'. All estimates have been calculated from other data in the report.

¹⁴⁷ Sources: NDNAD Reports, for 03/04 pp. 10, 18 and 22, for 04/05 pp. 6,10-11 and 16, for 05/06 pp. 24, 29 and 31-32, for 06/07 pp. 12, 19, 21, 24 and 26 and for 07/09 pp. 10-15.

¹⁴⁸ NDNAD Report for 2003/04 p. 22.

¹⁴⁹ Sources: NDNAD Report for 05/06 pp.12-13 and 35, for 06/07 p.31 and for 07/09 p. 28 and Scottish Government (2009) *Prison Statistics Scotland 2008-09 and Beyond*, p.16

Table 4.1: DNA database interoperability between Scotland and NDNAD: subject profile (sp) uploading and deletion. Note: ACPO sp retention policy was changed in December 2007. This change only affected the removal of English and Welsh sp from NDNAD.

Subject samples	2003/04	2004/05	2005/06	2006/07	2007/08	2008/09
Loaded (all sp)		521,117	715,239	722,464	591,028	580,174
Scottish sp Loaded (Note: no volunteer profiles)	42,000 (est.) (7% of total)	43,315 (7% of total)	46,856 (6.4% of total)	55,339 (7% of total)	NA	NA
Removals (E&W sp)	NA	NA	384 (est.)	488 (est.)	162	283
Removals (Scotland sp)	NA	NA	21,748	23,439	19,211	16,562
Removals (Scottish sp) as % of loads (in same year /previous year) (est.)			46.4%/50.2%	42.4%/50%	NA/34.7%	
Proportion of sp on NDNAD from Scotland at end of year (cumulative)	5.8%	5.5%	5.1%	4.8% (est.)	4.7%	4.6%

Table 4.2: DNA database interoperability between Scotland, Northern Ireland and NDNAD crime scene profile (csp) matches.

	2005/06	2006/07	2007/08	2008/09
All NDNAD csp matches with subject profiles	49,247	44,244	40,406	40,687
Excluding matches with csp from Scotland and NI	48,402 (est.) (only Scottish csp reported)	43,332 (est.) (only Scottish csp reported)	39,575 (est.)	39,697 (est.)
NDNAD csp matches with subject profiles from Scotland (as % of all)	1,388 (2.9%)	1,330 (3.1%)	1,119 (2.8%)	1,357 (3.4%)
NDNAD csp matches with subject profiles from NI (as % of all)	134 (0.3%)	36 (0.1%)	66 (0.2%)	131 (0.3%)
Scottish database csp matches plus NDNAD csp matches relating csp from Scotland	3,971(est.)	4,653 (est.)	N/A	N/A
NDNAD csp matches relating to csp from Scotland (as % of data in serial above)	845 (21.3%)	912 (19.6%)	787	880
Proportion of non-Scottish residents in prison custody in Scotland				3.6% (June 2008)

- 4.36. Some weight has been placed upon an observation in the Nuffield Council on Bioethics' report:

'The match rates between stored subject profiles and new crime scene profiles, which is 52%, can be contrasted with that of the Scottish DNA Database, which has a higher match rate of 68%. This demonstrates clearly that the more limited retention policy in Scotland does not negatively impact upon its subsequent match rates.'¹⁵⁰

It is becoming apparent from data published since the Report's publication that the comparative utility of the different retention regimes cannot be as clearly demonstrated as the NCOB believed at the time of its report.

- 4.37. Irrespective of changes in the data, such comparisons need to be treated with caution for two reasons. First, the two sets of match rates may be distorted by the interoperability of the two databases, how the match rates are calculated, and technical issues that may affect the generation and reporting of matches. Second, they are also likely to be affected by significant criminological or criminal justice organisational variations between the two jurisdictions.
- 4.38. The interoperability of the two databases may reduce the NDNAD match rate. As indicated above, all subject profiles typed in Scotland are uploaded to the Scottish database and NDNAD. However, a Scottish crime scene will only be uploaded to the NDNAD if it does not result in a match first on the Scottish database. As a consequence, a proportion of NDNAD subject profiles (the extent to which the proportion of Scottish subject profiles on NDNAD has changed little in recent years is indicated at Table 4.1) are unlikely to be matched against crime scenes. This view might not hold true if Scottish criminals were unusually mobile. This possibility cannot be discounted, but sixty years of research in the UK, USA and Australia indicates that burglary in particular - the volume offence that generates a high proportion of DNA crime scene profiles - tends to be committed within a small radius of the offenders home.¹⁵¹ Hence the annual NDNAD match rates may need to be discounted by a proportion of the 4.6% of its subject profiles currently from Scotland and possibly also those from Northern Ireland (1.2%).¹⁵² Comparisons may also be affected by technical issues in one jurisdiction. The failure by the FSS over an extensive period to load some 26,200 crime scene samples to the NDNAD delayed 1,168 match reports.
- 4.39. In any case, there is increasing convergence between NDNAD and Scottish database match rates. The latter appears to have declined slightly in recent

¹⁵⁰ *op.cit.* n.113, para. 4.52.

¹⁵¹ Wiles. P., & A. Costello, '*The Road to Nowhere: The Evidence for Travelling Criminals*', HO Research Study no.207, (Sept. 2000).

¹⁵² NDNAD Annual Report for 2007-09 p.15.

years from 68% in 2005/06¹⁵³ to 65% in 2008-09,¹⁵⁴ whereas the NDNAD match rate has steadily increased and averaged 58.7% in 2008/09.¹⁵⁵ It would be difficult to draw any reliable conclusions from this. The analysis of the differences between the operation of the two criminal justice systems and variations in criminological context would be a complex task. This justifies a note of caution about attempts to draw conclusions between the utility of the two retention regimes. For example, Scottish recorded burglary rates (per 100,000) have consistently been approximately half those in England and Wales.¹⁵⁶ As a result there will be significantly fewer opportunities (on a proportionate basis) to utilise DNA.

4.40. That Scotland has some 30% more police officers (per 100,000) and that the number of offences 'cleared up' per police officer in Scotland is four times greater than England and Wales¹⁵⁷ indicates fundamental differences in the patterns of recorded crime and the resources available within the criminal justice systems as a whole. As Table 4.3 (overleaf) indicates, in addition to significantly better 'clear up' rates, there appears to be much less reliance on the DNA database within the Scottish criminal justice system than in England and Wales in terms of the overall level of activity (as measured by recorded crimes and detections) in proportion to the number of profiles uploaded.

4.41. Despite the methodological challenges and the difficulties of obtaining data, a comparative and detailed study of the use of DNA in England and Wales, and Scotland should yield more information about cross-border cooperation, providing valuable insights into the consequences of different sampling and retention policies. The most promising area for research initially might be a fairly modest exercise. As can be seen from Table 4.2, Scottish crime scene profiles uploaded to NDNAD have a modest impact on NDNAD matches. If, however, these NDNAD matches are counted within the overall number of matches arising in relation to Scottish crime scenes (i.e. by adding them to Scottish database matches), it is notable that subject profiles from NDNAD contribute some twenty percent of Scottish matches. Research on a case by case basis into the circumstances relating to the latter set of data might improve our understanding of the effects of the different retention regimes and other issues. The disparity of impact on this scale is certainly unlikely to be caused by a disproportionate number of residents from England and Wales committing crimes in Scotland for which DNA is used for the purpose of detection. It is much more likely to be influenced by different sampling and retention policies.

¹⁵³ NDNAD Annual Report for 2005-06 p.24.

¹⁵⁴ SPSA Annual Report and accounts 2008-09 p.21.

¹⁵⁵ NDNAD Annual Report for 2007-09, p.33.

¹⁵⁶ European Source Book 2006, Table 1.2.1.11.

¹⁵⁷ Approximately 319 per 100,000 resident population in Scotland and 261 in England and Wales: calculated (as FTEs) from The Scottish Government (2009) Police Officer Quarterly Strength Statistics Scotland, 31 December 2009, using the figure for December 2008, ACPO Police service strength in England and Wales at March 2008 (data at March 2008) and ONS 2008 mid-year population estimates.

Table 4.3: Recorded crime and subject sample uploads, 2004/05-06/07.¹⁵⁸

	2004/05 (2004 for English stats.) thousands	2005/06 (2005 for English stats.) thousands	2006/07 (2006 for English stats.) thousands
England & Wales			
Offences recorded	5,641	5,557	5,428
Offences 'detected'	1,441	1,516	1,374
Subject profiles (sp) loaded	447	668	629
Ratio of offences / offences detected to sp loaded	11.8/3	8.3/2.3	8.6/2.2
Scotland			
Offences and crimes	1,077	1,018	1,026
Offences and crimes cleared up	791	749	765
Sp loaded	43	47	55
Ratio of offences and crimes / offences and crimes 'cleared up to subject profiles loaded	24.9/18.3	21.8/16	18.5/13.8

The interplay of policy & technological development

4.42. Johnson and Williams' review of the use of DNA in Scotland highlighted differences in the culture of the Scottish system and views about the utility of DNA databases to those in England and Wales. They stressed how important distinctions were rooted in a Scottish Law Commission report in 1989 and the Royal Commission on Criminal Justice in England & Wales report in 1993:

'Both commissions focused on the essential need to allow the police to use genetic technology in a 'balanced and proportionate' way that would ensure the protection of individual rights and civil liberties as well as maximize the potential for criminal detection. Both commissions also placed great emphasis on the potential for DNA testing to exonerate individuals during police investigations, coupled with the idea of DNA as a definitive forensic method which could incorporate high statistical probabilities of certainty (and thus a form of 'objectivity') into legal proceedings. However, they differed in how this technology should be translated into practices for policing.'

¹⁵⁸ Sources: Ministry of Justice (2008) *Criminal Statistics: England and Wales 2007*, Figure 1.1, p.10, National Statistics for Scotland (2009) *Criminal Proceedings in Scottish Courts, 2007/08*, Chart 2, p.7 and NDNAD reports for 2004/05, pp.10-11 and 22, for 2005/06 pp.25, 29 and 32, for pp.12, 19 and 26.

- 4.43. The Scottish Commission, when considering the balance needed to enable DNA to work effectively, and the rights of the individual, proposed that the power to take samples without consent 'should not include anything which involves going inside a person's body'. This recommendation was not reflected in legislation. The 1995 Criminal Procedure (Scotland) Act allowed for the taking of a mouth swab without consent, reflecting the approach taken in the Criminal Justice and Public Order Act 1994. The only distinction was that this had to be authorised by an officer with a rank no lower than inspector. The 2003 Criminal Justice (Scotland) Act removed this requirement.¹⁵⁹
- 4.44. Irrespective of the change in the law, ACPOS policy still places considerable stress on a police constable's individual judgment. It advises against the universal sampling of arrestees. Instead this should only happen where a person has been arrested or detained for crimes of violence, sexual offences or theft or, at the arresting officer's discretion, it is deemed 'appropriate'.¹⁶⁰ This could be explained, in part at least, by the minimal central government support for expanding the use of DNA, but there may equally be something in Scottish policing culture or a different perception of the value of the utility of the DNA database. Certainly some forces were reluctant to make use of the same legislation to retain samples relating to individuals who had not been convicted. When reviewing Scottish DNA retention policy, Fraser found that by December 2007, five of the eight Scottish police forces had still not made use of the extended power of retention that had come into effect.¹⁶¹
- 4.45. The technological development issues are easier to discern and it is possible to see how they might have contributed to a different approach. The deliberate restriction of sampling on arrest reflected a similar policy in England and Wales that prevailed while the FSS had insufficient capacity to undertake such work.¹⁶² This approach was only reversed by the then Prime Minister's announcement of the DNA Expansion Programme, the aim of which was to have on record the DNA profile of 'every known offender'. This new policy, together with the ring-fenced central government funding, meant the volume of subject profiles uploaded to NDNAD trebled during 2000–2005.¹⁶³ The history of the use of DNA in Scotland shows a similar pattern of initial capacity constraint and subsequently greater encouragement to obtain DNA on arrest once analytical facilities had been automated and capacity had been brought back into balance with potential demand.

¹⁵⁹ Johnson, P. and Williams, R. 'DNA and Crime Investigation: Scotland and the 'UK National DNA Database' *Scottish Journal of Criminal Justice Studies* 10: 71-84

¹⁶⁰ NDNAD Report 2004/05 p.8.

¹⁶¹ Fraser, J. (2008) *Acquisition and Retention of DNA and Fingerprint Data in Scotland* p.14 as published in September 2008 at www.scotland.gov.uk/Consultations/Current .

¹⁶² Blakey, D. (2000) *'Under the Microscope'*, (London: Home Office), p.23.

¹⁶³ Home Office (2006) *DNA Expansion programme 2000-2005: Reporting Achievement* (London: Home Office), p.3-4.

4.46. The introduction of DNA sampling had been delayed north of the border so that by the time Scottish forces were submitting samples to the FSS for analysis there were already major backlogs. This meant that the proposed processing times offered to Scottish forces was unacceptable. Only then was it decided to create a separate Scottish database populated by profiles from Scottish police laboratories.¹⁶⁴ Thereafter investment in automation was much slower though its introduction was soon followed by expressions of concern about the level of 'forensic capture'. The SPSA reporting that:

'A marketing campaign has been introduced to increase awareness and to promote the capture of criminal justice samples and fingerprints by police officers. Posters have been designed and circulated via ACPOS to custody suites across Scotland promoting the message of forensic capture to ensure our DNA and Fingerprint databases are as up to date as possible in order to provide more opportunity for successful hits and identifications.'¹⁶⁵

4.47. The sampling and retention of child profiles also provides an insight into different legal, cultural factors. Although few children are involved and the ages of criminal responsibility are different, data suggest that the Scottish legal system has been more willing to authorise the collection of bioinformation relating to young people less than ten years of age than in England and Wales.¹⁶⁶ Legislation going through the Scottish parliament will expand retention to children who admit guilt under the Children's Hearing System, but the age of criminal responsibility is to rise from 8 to 12 years.

4.48. There is greater consideration of the Scottish position in Chapter 6, but conclusions from this brief consideration of the Scottish arrangements include the interoperability of NDNAD and the Scottish database, together with the ability of the forensic services of the two administrations and Scottish criminal justice colleagues to manage different retention regimes on a large scale as indicated in Table 4.1, is clear evidence that forensic cross-jurisdictional cooperation can be successfully managed on a large scale despite legal differences. While this report identifies some gaps and lack of consistency in the data and suggests where research is urgently needed, the scale and detail of the interoperability analysis indicates that NDNAD has set an example of greater openness nationally and internationally for criminal justice databases, including the exchange of information about fingerprints, and possibly genetic collections in the genetic research and health fields.

¹⁶⁴ NDNAD Annual Report 2004/05 p.6

¹⁶⁵ SPSA Annual Report and accounts 2008-09 p.21.

¹⁶⁶ In 2008/09 the number of profiles for children under ten on NDNAD was 96 for England and Wales and 33 for Scotland, which if recalculated as per 100,000 population corresponds to 0.18 and 0.63 respectively. NDNAD Annual Report 2008/09.

4.49. Finally there is some evidence to support the contention made in this report that a margin of appreciation based on no more than a survey of legislation is a possibly more fragile basis for reaching views on proportionality than is suggested in *Marper*. Scotland may have achieved a very balanced approach to retention issues that still need to be settled south of the border. This appears to have been as much a chance outcome, as one of good professional and political judgment. It is far from clear however, from reading recent debates at Westminster that what we would argue is the defining characteristic of Scots law in this area – the exercise of individual discretion - has been fully understood.

Validity, technological development and DNA sample retention

4.50. Discussion about validity during the seminars caused us to focus on three issues in particular:

- False or adventitious matches, false eliminations and sample retention;
- The challenge of ensuring the validity of dactyloscopic information;
- The foreseeable technological obsolescence of the SGM+ multiplex.

The risk of these problems materialising is greatest when information is exchanged between foreign jurisdictions, but is present when poor material has been recovered from a crime scene and when using old records created with either a lower discriminating power or to poorer technical standards.

False or adventitious matches, false eliminations and sample retention

4.51. Different modes of individualisation based on bioinformation give rise to different scientific and professional challenges, but common to all is the recognition that mistakes have unacceptable consequences for individuals and confidence in the criminal justice system. These issues are explored more easily by an examination of the forensic use of DNA because of the greater availability of information, but examples and specific points relating to fingerprints are also included where possible.

4.52. Within common law jurisdictions, debate about the validity of DNA matches has focused on adventitious and false matches.¹⁶⁷ An adventitious match is when the DNA profiles of two individuals, who are not identical twins, match. This is theoretically quite a rare occurrence within a DNA typing or multiplex that has a sufficient discriminating power. The risk is minimised chiefly by using a marker or typing system with an adequate number of loci for the size of the population of the database or network of databases from which a match is being sought.

¹⁶⁷ See especially Lynch, M. Cole, S.A., McNally, R. and Jordan, K. (2008) *Truth Machine: The Contentious History of DNA Fingerprinting*, Chicago and London: Chicago University Press.

With the UK SGM+ multiplex (10 loci plus Amelogenin) the chance of an adventitious match (for people who are not siblings) is reported to be 1 in 1,000 million.¹⁶⁸ In this report another term is used in respect of both DNA and fingerprints: a false match. This describes a more commonplace situation when there initially appears to be a match, but closer examination shows that result to be invalid. A false DNA match is likely to be the result of one or more of the following potential sources of error:

- Insufficient loci available for analysis from degraded DNA material recovered from the crime scene resulting in an inability to take advantage of the maximum discriminating power of the marker or typing system;
- A misattribution of the source of a loci reading to a specific individual when cellular material recovered from a crime scene belongs to more than one person (a 'mixed sample');
- An attempt to match an incomplete set of loci by using only the small number of loci it has in common with different marker or typing systems (e.g. during international exchanges or when samples generated by using the current multiplex system are compared with profiles produced by previous multiplexes that are less discriminating).

The third complication is both a source of error in its own right and a factor that can compound problems arising in respect of the other two. Genetically an adventitious match is a reliable result within the scientific parameters of the typing system, but a false match is methodologically unreliable. For the purposes of individualisation within legal proceedings both are invalid.

4.53. During seminars experts referred to the regular and beneficial exchange of fingerprint data between Austria and Germany over many years. However, very similar problems can occur in respect of fingerprint matches, particularly when what has been recovered from the crime scene is incomplete, degraded by decay or fire, distorted when the trace was made, or has been searched for by more than one proprietary algorithm. Problems can also arise from the use of poor tenprints obtained manually using ink and paper. Despite the extensive use of modern technology in wealthier countries, most tenprint records in use today were obtained manually and this century old method is still the main method used for enrolments, within criminal justice systems at least, in most countries of the world. Problems are compounded when the quality of an image is reduced in transmission internationally between different fingerprint bureaux.

4.54. It was suggested during seminars that equal attention should be paid to false eliminations, which arise for the same reasons as a false match. Indeed a risk is present whenever DNA analysis is used if there are only a small number of loci in common during a search involving profiles obtained from a multiplex with

¹⁶⁸ NDNAD Annual Report 2003-04, p 33.

a lower discriminatory power (within the UK, the SGM system), or during international searches involving multiplexes with a limited number of loci in common. It is most likely to occur when a crime scene sample is degraded and a limited range of alleles can be amplified. Problems may also arise because of variation in PCR when different typing systems are used. One of the kits used may not have resulted in one of a pair of alleles being amplified to a detectable level, but the other system may have amplified both alleles.

- 4.55. The limited evidence available from US fingerprint proficiency testing suggests that false eliminations may occur on a smaller scale. Reports of the proficiency testing undertaken by the American Society of Crime Laboratory Directors indicate that 8% of the latent prints deemed by those conducting the tests to be inadequate for identification were not so marked. In contrast, 2% of the latent prints deemed adequate were scored as unsuitable for individualisation.¹⁶⁹
- 4.56. While the problem of false identifications is generally acknowledged, the consequences have not necessarily always been analysed. For example, the Human Genetics Commission suggested that a crime scene from Lewisham is more likely to be linked to a local resident, than a resident of Lisbon or Lugano.¹⁷⁰ Hence, the investigator will know that the inquiry should concentrate on the candidate match with a local resident, rather than one identified via, say by a six loci match (the European and Interpol standard set) elsewhere in Europe. In reality this would indeed be the case with a full SGM+ match (crime scene to personal profile stored on NDNAD). In the absence of such a clear result, it may be inappropriate to close minds to a possible foreign connection. Criminal investigation within Lewisham has to take account of the nature of its resident population. ONS research indicates that by 2008 almost a third of Lewisham residents were not UK born, although Lagos had much greater links with that borough than Lisbon or Lugano.¹⁷¹
- 4.57. During the seminars it was acknowledged, as the Human Genetics Commission suggested, that investigators will often be able to eliminate adventitious or false matches fairly easily because it will be apparent with minimum checking that the individual concerned has nothing to do with the crime under investigation. Sometimes however, the issues may not be easy to resolve. This can result in considerable intrusion into the private life of an individual. What has not been recognised is that such a situation would be the equivalent to the suspicion initiated by a close non-match obtained by the use of familial searching. The accidental and unknown nature of the linkage with the investigation however, means that none of the safeguards deemed essential for familial searching will

¹⁶⁹ Pyrek, K.M. (2007) *Forensic Science Under Siege* (Burlington MA: Elsevier Academic Press), p. 269.

¹⁷⁰ Human Genetics Commission, (2009) *'Nothing to Hide, Nothing to Fear'* London, Department of Health pp70-71.

¹⁷¹ Ellis, A. Population Trends 135, Spring 2009: UK resident population by country of birth, at <http://www.statistics.gov.uk/articles/populationtrends/PT135POPCOBARTICLE.pdf> accessed 7 March 2010.

be in place. In the worst case scenario, someone may be trapped in a nightmare situation because of a combination of a false match or near match and circumstances judged to corroborate an unreliable biometric result.

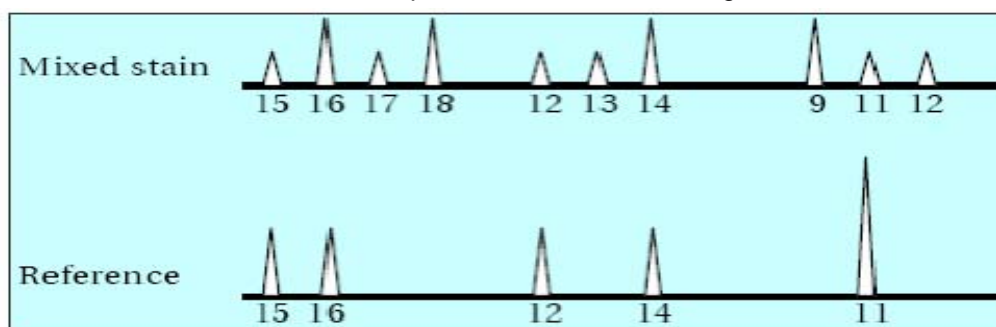
- 4.58. Dactyloscopic cooperation resulted in the most well known case of this kind: that of Brandon Mayfield. A US born lawyer and former Army lieutenant, Mayfield received \$2 million in compensation from the FBI for what he described as the 'horrific pain, torture and humiliation' caused to himself and his family as a result of a false fingerprint match.¹⁷² He was detained (initially in a single cell for up to 22 hours a day) after the FBI claimed that his prints matched those found on a bag of detonators in Madrid following the 2004 train bombing. This result was challenged by the Spanish police. The FBI examiners later acknowledged that they did not re-examine their initial match decision as carefully as they should have done. They knew by that time that Mayfield was a convert to Islam, had an Egyptian wife and had represented a convicted Islamic terrorist in a child custody dispute. An official investigation largely exonerated the FBI examiners, focusing on the problems of dealing with 'confusingly similar prints' identified by an automated database search, as an 'unusually close non-match'. It concluded however, that the examiners had been willing to 'accept an extraordinary set of coincidences' in explaining their identification, and that internal reporting arrangements within the FBI had resulted in 'implicit pressure' on the examiner to declare a positive identification 'when faced with a difficult comparison in a case involving a particularly heinous crime'.¹⁷³
- 4.59. The reverse situation – a false elimination - may be equally damaging for the administration of justice. A scientific or professional inability to match bioinformation from the crime scene with data held under a different system may result in an investigation being discontinued or being focused on the wrong suspect simply because of a vague circumstantial fit with the limited information about the crime. From our analysis of the political ambitions for the greater exchange of forensic bioinformation internationally, it is reasonable to assume that in the absence of technological, organisational and professional improvements, that this is likely to be a growing problem in the future. It may be however, that organisational improvement could be achieved simply through investment in information technology, including automatic database searching. This could be a costly mistake. With the increasing horizontal integration of criminal justice data, staff currently working on international cooperation could be overwhelmed by data and, as was seen in the Mayfield case, in major investigations face considerable pressure to confirm 'near close matches'.

¹⁷² Lichtblau, E. New York Times, 30 November 2006, 'US Will Pay \$2 Million to Lawyer Wrongly Jailed', at http://www.nytimes.com/2006/11/30/us/30settle.html?_r=1, accessed 6 March 2010.

¹⁷³ US Department of Justice (2006) Office of the Inspector General Oversight and Review Division, A Review of the FBI's Handling of the Brandon Mayfield Case, especially pp.7, 9,11-12 and 20-21, at http://www.justice.gov/oig/special/s0601/PDF_list.htm accessed 6 March 2010.

- 4.60. The potential widespread distribution of automated searching for matches to latent print matches (under Prüm this could yield 10 closest matches from 26 countries), could quickly produce candidate match ‘overload’. Greater reliance on automated matching however, could exclude a potential match by not putting it on the list of, say, ten candidate matches or closest near matches. This might incorrectly eliminate the offender from the inquiry. Similar problems were anticipated in respect of DNA by the ENSFI DNA Working Group in 2009. They concluded that while the European Standard Set of Loci are sufficient for the present ‘occasional exchange of DNA-profiles between countries’, the much higher volume of exchanges of DNA-profiles made possible by the Interpol DNA-database and the Prüm Treaty means that the chance of adventitious or false matches will no longer be negligible, and may become significant.¹⁷⁴
- 4.61. The ENSFI report also provided clear examples of the risk of invalid results because of misplaced reliance on automation alone or inadequate software within an automated searching system. Some DNA-databases, such as CODIS, contain mixed DNA-profiles and can be searched internationally. This can be very helpful when investigating serious crimes. A numerical match between a reference sample and a mixed profile however, must always be visually checked against the plots of the DNA-profile because a numerical match may not be a real match as shown in Figure 4.1. In addition, when two profiles have been generated by using different multiplexes there is a risk of missing a match due to the occurrence of so-called ‘null-alleles’. This is the result of a sampling variation between two multiplexes resulting in the failure by one to amplify an allele. One system might incorrectly detect only one allele present in the sample (apparent homozygote or two identical alleles at a given locus), but the second may have detected two alleles (apparent heterozygote or two different alleles at a locus). The presence of a null-allele is identified by observing the unexpected low peak height on the plots of the DNA profile of the apparent homozygote, but this requires an attentive DNA-analyst or intelligent allele-calling software.¹⁷⁵

Figure 4.1: Example provided by the ENSFI DNA Working Group illustrating how three loci of a mixed stain and a reference sample which match on a numerical basis can be seen not to match when the mixed profile is attributed to a single individual contributor



¹⁷⁴ ENSFI (2009) DNA-Database Management Review and recommendations at http://www.ensfi.eu/get_doc.php?uid=345, accessed 6 March 2010, p.8.

¹⁷⁵ *ibid.* pp.12-13 and 8.

- 4.62. The only effective way of dealing presently with invalid results when using DNA appears to be, as recommended by ENSFI, that of retaining cellular material for the same period as the profiles. It is also important to ensure that there are sufficient DNA and fingerprint analysts to scrutinise candidate matches in conditions where they are not placed under direct investigatory pressures. This is clearly not a satisfactory long-term solution and many organisations have significant privacy concerns. There are also cost implications. An interim option would be to bring the UK into line with best practice in North America, where demographic information is not sent to any FBI or RCMP forensic laboratory that analyses personal profiles. Cost reduction ultimately depends on considerable technological progress (considered below). In the meantime, samples are being retyped extensively when matches are identified between Germany and the Netherlands during their trials of the Prüm arrangements. This extra work adds significantly to cost and speed, making it less effective for finding forensic leads. However, these considerations may not detract from the possibly greater benefits from not unnecessarily sending demographic details to laboratories, a practice that opens possibilities for abuse and security lapses, and has been criticised by those running the laboratories themselves.
- 4.63. Similar obstacles can be anticipated in the progress of UK cold case review work as degraded crime scene material is reanalysed using a new multiplex. In either instance the problems of ensuring acceptable sample storage and the cost of retyping personal profiles might prove, on balance, to be acceptable. They need to be compared with the burden of potential investigative or legal work to avoid or respond to legal challenges during a trial if all candidate matches had not been exhaustively investigated for elimination purposes. Also, a judgment needs to be made about the potential impact of sample destruction. Not being able to follow-up 'near matches', and the ability to reanalyse old crime scene material, may negatively impact upon effectiveness as a result of foreseeable technological advances.
- 4.64. The analysis of these issues should take account of the existence of a proven option for reducing sample storage costs. The present storage of samples at -20 degrees Celsius could be replaced by FTA paper storage in ambient conditions. Regrettably it can be seen from the Impact Assessment published to support the Crime and Security Bill 2010 that the consideration given to this issue by the Government did not identify ambient storage as an option:

'It costs around £0.90/year to store a DNA sample in a fridge. Under the option of destroying all DNA samples, this cost would not occur. Given the large number of samples that would need to be removed we have estimated a saving of around £5.2m (one-off) and £7.7m/year.'¹⁷⁶

¹⁷⁶ Home Office (2009), *Impact Assessment of the implementation of the S & Marper ECtHR judgment regarding DNA profiles, DNA samples and fingerprints retention* published at www.crimereduction.homeoffice.gov.uk/crimeandsecuritybill/

- 4.65. The impact assessment acknowledged however, that the options for dealing with this issue had only received limited analysis during the consultation stage:

‘While most respondents failed to differentiate between samples and the profiles which are derived from them, where they did, there was strong support from the public and civil liberties groups for the proposal to destroy samples. However, some caution was expressed by policing and prosecutorial organisations in terms of possible operational and evidential implications’.¹⁷⁷

The Government also admitted that re-sampling ‘may not be practical or appropriate in a large number of cases’ should new techniques be developed to extract more information from crime scene samples or assistance be requested internationally. It accepted that investigations might fail both domestically and abroad due to the inability to produce the original sample.

Ensuring the validity of dactyloscopic information

- 4.66. As a forensic technique grounded in professional expertise rather than replicable and independently verifiable methodology, dactyloscopic examination faces major challenges in the light of the McKie case in Scotland,¹⁷⁸ and the Brandon Mayfield case in the USA. As a result of problems documented in the NRC 2009 report ‘*Strengthening Forensic Science in the United States: A Path Forward*’, there may be a new round of challenges to fingerprint evidence and other experienced based forensic disciplines. It is suggested in that document that there now needs to be a clearer understanding of the basis for valid fingerprint matches, together with research into causes of error and error rates.

- 4.67. The massive expansion in the exchange of such information for border control purposes, as well as the less dramatic growth of cooperation in the course of traditional criminal investigations, means that new fingerprint standards for establishing the validity of matches need to be applicable globally. The ENFSI fingerprint working group is seeking to establish what is being done in the different EU countries. Their analysis will cover national identification methods, the testing of procedures and the assessment of personal competency. The ENFSI fingerprint group and the International Association of Identification (IAI) have links, but it was suggested that both organisations need to achieve greater visibility and wield more influence internationally.

¹⁷⁷ *supra*.

¹⁷⁸ The Scottish Fingerprint Inquiry was established with the following terms of reference:

- ◆ To inquire into the steps that were taken to identify and verify the fingerprints associated with, and leading up to, the case of *HM Advocate v. McKie* in 1999, and
- ◆ To determine, in relation to the fingerprint designated Y7, the consequences of the steps taken, or not taken, and
- ◆ To report findings of fact and make recommendations as to what measures might now be introduced, beyond those that have already been introduced since 1999, to ensure that any shortcomings are avoided in the future. For current developments see: <http://www.thefingerprintinquiryscotland.org.uk/inquiry/21.html>

- 4.68. During seminar discussion, developing a probabilistic basis for fingerprint identification or perhaps reaching agreement on a numeric standard were seen as the two most promising ways forward. This would enable the fingerprint community to follow the lead of ENSFI in introducing proficiency testing and audits. Whatever approach is adopted, it would be necessary to ensure that the transition to more highly complex and statistically demanding approach is made intelligible to existing practitioners whose existing working methods and professional expertise will undergo a major change. Dror and Mnookin have considered more systematically than was possible in our discussions, the increased risks of examiners making erroneous identifications because of the scale and speed of automated database searching. This arises from the increased chances that automated searching will produce an increased number of candidate matches based on incidental similarities and that some of these may be an 'artifact both of the relative similarity of the patterns being compared and of the human cognitive architecture involved in pattern matching'.¹⁷⁹
- 4.69. Technical problems relating to the transmission of data and the preparation or presentation of information for analysis theoretically at least present fewer problems. The transmission of good digital images is critical. It should be possible to reach an international agreement and introduce changes quickly subject to available funding. This could include the minimal pixel quality of exchanged images and the replacement of ink and rollers with digital image capture such as LIVESCAN which is used in UK custody suites. However, it was noted that little progress had been made internationally other than a very limited agreement dealing with the file format for transmitting information.
- 4.70. Automated search systems generally decrease reliance on individual decision-making while reducing costs and speeding up database searches. While the manual scrutiny of candidate matches remains essential when dealing with latent marks, it is less important when comparing a LIVESCAN reading from someone brought into custody with an equally good set of tenprints on NAFIS. The introduction of 24/7 automation has made a huge difference in the ability of the police to verify the identity of persons in custody despite most UK fingerprint bureaux operating only five days a week.
- 4.71. The downside to the history of technological development in this field has been how this has been based on the ad hoc development of different proprietary search and image capture systems. Often different systems, sometimes even different versions of the same system from a single manufacturer, are not interoperable. Similarly, different algorithms used to retrieve stored prints in accordance with a specific input map of features may require fingerprint

¹⁷⁹ Dror, I.E. and Mnookin, J.L., 'The use of technology in human expert domains: challenges and risks arising from the use of automated fingerprint identification systems in forensic science', *Law, Probability and Risk*, Advance Access, published January 22, 2010, p.21.

examiners to learn system specific ways of annotating features on a latent print in order to maximise the chances of a successful identification. This situation was compared unfavourably in the NRC report with the high levels of interoperability achieved for other distributed information networks, including banking systems, such as ATM machines. The successful development of such IT systems requires 'finely crafted and agreed standards and protocols'. This, the report concluded, would require strong, high level support from government policy makers, and additional public funding.¹⁸⁰

4.72. Seminar discussions also acknowledged that there may also be development aid, IPR, and strategic procurement issues that need to be addressed for the benefit of developing and middle income countries. Some have recently tried to consider systematically the increased risks of examiners making erroneous identifications because of the scale and speed of automated database searching. This arises from the increased chances that automated searching will produce an increased volume of candidate matches that are based on incidental similarities and that some of these may be an 'artefact both of the relative similarity of the patterns being compared and of the human cognitive architecture involved in pattern matching'.¹⁸¹

4.73. It is unclear within the UK how strategic coordination has taken place, even in terms of basic system design. The Home Office decided to use LIVESCAN tenprint scanning for subject enrolment for identity cards and passports. This is in contrast to enrolment on IDENT1, where the standard is based upon rolled prints. Both choices probably made sense in isolation. LIVESCAN enrolment is likely to be quicker and cheaper than rolled prints, but rolled prints was the standard judged necessary for comparisons with latent prints within the criminal justice system. The critical question is whether, if or when, the identity card and passport tenprints are accessed for criminal justice purposes, they will be suitable for this purpose? This may simply be a matter of ensuring a more intensive scrutiny of potential matches or near close matches when prints obtained outside the criminal justice system are compared with latent prints. At a minimum, there appears to be a prime facie case for interdependent assurance that in such a situation adequate safeguards are in place. One aspect that may have to be capable of being monitored is that there are a sufficient number of competent experts in place to scrutinise automatic search results, so that such reports can be properly verified or caveats attached before being passed to investigators.

¹⁸⁰ National Research Council of the National Academies (2009) *Strengthening Forensic Science in the United States: A Path Forward*, Washington DC: The National Academies Press, pp.269-278.

¹⁸¹ *op.cit.* n.179, p.21.

The foreseeable technological obsolescence of SGM+

- 4.74. During seminar discussion there was general agreement that the variety and differing configurations of multiplex introduced over a decade ago are barriers to efficient and cost-effective use nationally or exchange internationally. The systems used most frequently, especially in the UK and in countries from where the majority of known serious offenders in this country originate, are set out overleaf in Figure 4.2. Within the European Union this problem is to be dealt with in the medium term by introducing five new markers. These loci (Next Generation Multiplex - NGM) have been developed for two reasons. Firstly, they provide more discriminating power as national databases grow in size and are searched more frequently alongside other national databases. Secondly, they have a low molecular weight and will be more successful when used to analyse degraded samples. This multiplex was introduced at the end of 2009 and their use in all member states by November 2011 was recommended in a Council Resolution on 30 November 2009.¹⁸²
- 4.75. The cost of switching will reflect not only higher analysis costs (extra reagents and additional processing), but also software upgrades for the NDNAD and other DNA (provider and Interpol) databases. We were told that within the EU it was estimated the five new loci would ensure sufficient levels of discrimination for another five years.

¹⁸² EU Council Resolution on the exchange of DNA analysis results (2009/C 296/01).

Figure 4.2: Analysis of loci used in DNA multiplex in the countries with the most criminological links with the UK.

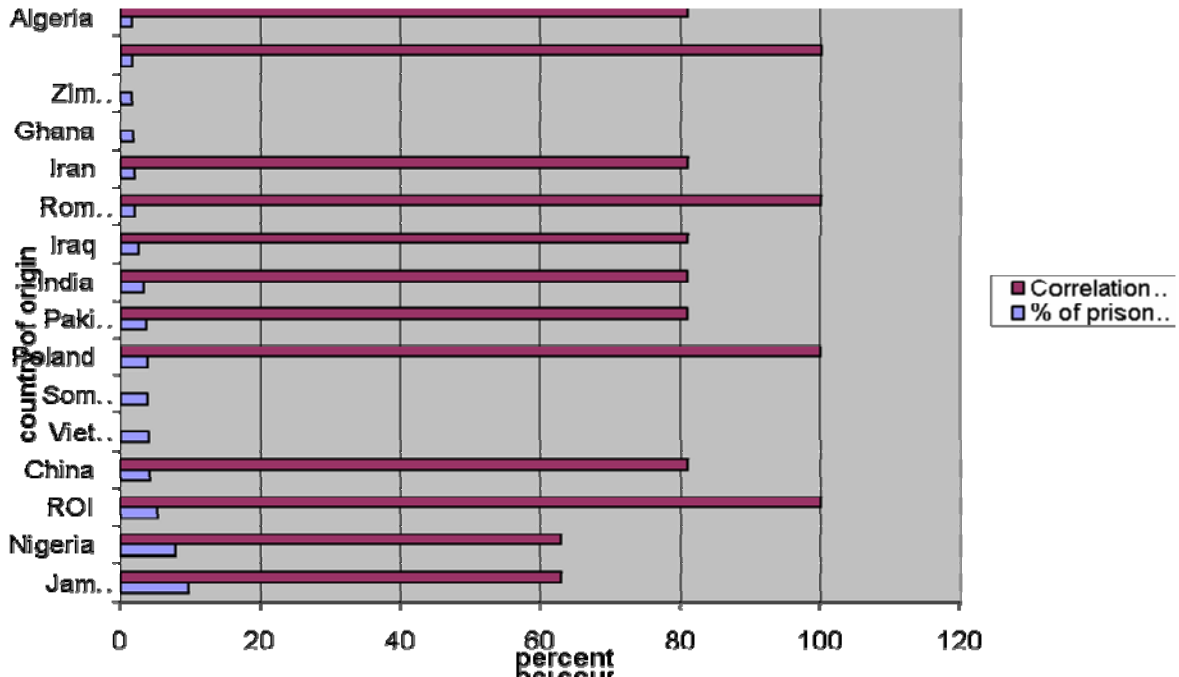
	CODIS	Identifier	Type 15 (Sinofiler)	P16	Pp2	Pp1	Pro+	SGM+	ENSFI/Interpol standard set
D6			•					•	
D19			•					•	
D2S1338								•	
D19S433								•	
D5S818	•	•	•	•		•	•	•	
D7S820	•	•	•	•		•	•	•	
D13S317	•	•	•	•		•	•	•	
CSF1PO	•	•	•	•		•	•	•	
TPOX	•	•		•	•	•		•	
D16S539	•	•	•	•	•	•	•	•	
D18S51	•	•	•	•	•	•	•	•	•
D8S1179	•	•	•	•	•	•	•	•	•
D3S1358	•	•	•	•	•	•	•	•	•
TH01	•	•	•	•	•	•	•	•	•
VWA	•	•	•	•	•	•	•	•	•
FGA	•	•	•	•	•	•	•	•	•
D21S11	•	•	•	•	•	•	•	•	•
Penta D			•	•				•	
Penta E				•				•	
Amelogenin		•	•	•			•	•	
Additional ENSFI standard set									
D1S1656	?							?	•
D2S441	?							?	•
D10S1248	?							?	•
D12S391	?							?	•
D22S1045	?							?	•
Correlation with SGM+ (?/11)	8	9	8	9	7	3	7		7
Correlation with CODIS (?/13)		13	11	13	8	8	9	8	7
Correlation with Type 15 (?/15)	11	12		13	7	7	7	10	8

4.76. For the UK the loci issue can be summarised as follows:

- Its multiplex, SGM+, is already technologically obsolescent, but adding the five NGM loci could considerably reduce the risk of false matches, adventitious hits or false eliminations (domestically as the NDNAD grows and internationally as the volume of data exchange increases). It would also increase the potential value of reinvestigating older crimes, particularly murders and serious sexual offences.
- Even the next upgrade, by adding the five NGM loci, may only be of value for about another five years.
- Even if the UK remains in step with other EU member states the origin of the most serious criminals known to have committed offences in this country means that in many cases the multiplex used in their home country

and the UK do not have sufficient common loci to be confident of the quality of any exchanged information or evidence being reliable. This problem is illustrated at Figure 4.3.

Figure 4.3: The correlation (proportion of loci in common) of SGM+ with the multiplex used (where known) by countries with 200 or more citizens in custody in England and Wales at 31 December 2008.



- 4.77. International data indicates that SGM+ is a significant multiplex globally and within the EU. Investment in five new loci is probably a good medium term option. The issue that needs to be grasped now is what should be available in five years time? In attempting to forecast possible trends the much closer convergence of China (the fastest growing DNA database) and the USA (the world's largest DNA database) is probably the most strategic public policy issue relating to the technological development of DNA multiplexes that the governments of the UK and EU, together with the Council and Commission have to address. China originally used 'Identifiler' (equivalent to CODIS plus Amelogenin), the same multiplex as Hong Kong, but some time ago a new kit was developed with 15 loci: Type 15 or 'Sinofiler'. This is identical to Identifiler except for the replacement of two CODIS loci and the addition of two loci not used in other systems. At present it is believed that half the profiling work in China is carried out with Identifiler, but eventually all analyses will use Sinofiler.
- 4.78. The problem with the development of new multiplex within Europe is the risk of being significantly out of step in terms of access to the benefits of technological development; more effective international law enforcement cooperation; and commercially with the predominant systems used elsewhere in the world. Links

with medium income countries through the Commonwealth will make no difference. South Africa is the key country within sub-Saharan Africa for undertaking DNA analysis for other countries in its region. It uses Pro+ (seven common SGM+ and Identifiler loci, together with an additional three Identifiler loci). Jamaica may be the country of origin for the largest proportion of foreign nationals (predominantly male) in English prisons, but the impact of Jamaican crime (as indicated by the deportation of Jamaican citizens for firearms and violent offences) is greater in the USA rather than the UK and Jamaica uses Powerplex systems not SGM+.

- 4.79. ENSFI works with the relevant US and Australasian bodies, SWGDAM (Scientific Working Group on DNA Analysis Methods) and SMANZL (Senior Managers Australian and New Zealand Forensic Laboratories), but it is quite difficult to co-ordinate and collaborate effectively with no regular funding and, as a voluntary organisation for forensic providers, cannot have a formal mandate to seek to promote coordination with North America or China. It exists on the basis of minimal public funding limited to travel expenses and small research projects, and no political support. Hence, progress in developing new multiplex had only been possible because of the goodwill of scientists and the advantage for two biochemical companies of ENSFI cooperation in developing a new product that might be marketed beyond Europe. There is some optimism that other countries will consider adopting the 5 loci that have been developed by ENSFI when expanding their core loci. There is however, a major technical barrier for achieving any kind of multiplex that would provide a more reliable overlap between the various CODIS based multiplex and the different systems developed in Europe. The kind of 20 loci multiplex that might make this possible would require new biochemistry, at present it is technologically impossible to go beyond a 15 or 16 loci system.
- 4.80. The absence of coordinated EU national or Commission strategic involvement also results in over dependence on commercial biochemistry. The absence of public funding to create a public sector IPR for the new markers reflects the weakness of the ENSFI, as the only EU forensic science body. We were advised that even attempts to reduce analytical costs by reducing the market dominance of the two dominant companies appear to have been blocked by legal action to prevent a new company entering the market. On the other hand, the limited number of commercial companies in the market has at least prevented an even greater proliferation of multiplex systems. There is also a more general economic issue arising in respect of IPR. For international cooperation to work and to assist poorer countries achieve a modern criminal justice system, it must be possible for less wealthy countries to access DNA profiling. This problem needs to be recognised as being akin to the issue of access to generic drugs for developing and middle income countries.

Conclusion

- 4.81. While information is scarce, the amount of cooperation involving the use of DNA appears to be occasional even when investigating serious crimes. Within the European Union this might change as a result of the Prüm Treaty, although the Council of the European Union has already sought to restrict the extent of future searching under Prüm, presumably to prevent analysts being overwhelmed by search requests and the need to verify results.
- 4.82. The interoperability of NDNAD and the Scottish database, together with the ability of the forensic services of the two administrations and Scottish criminal justice colleagues to manage different retention regimes on a large scale is clear evidence that forensic cross-jurisdictional cooperation can be successfully managed on a large scale despite legal differences. While this report identifies some gaps and lack of consistency in the data and suggests where research is urgently needed, the scale and detail of the interoperability analysis indicates that the NDNAD has set an example of greater openness nationally and internationally for criminal justice databases, including the exchange of information about fingerprints, and possibly genetic collections in the genetic medical research and health fields.
- 4.83. While the issues of validity, technological development and sample retention have been considered in the context of international cooperation, it is important to bear in mind that transnational crime is only a small proportion of recorded crime, particularly those offences where bioinformation can be obtained from a crime scene.¹⁸³ The advantage of considering such issues however, serves to identify some of the key strategic issues that will need to be addressed for domestic reasons and acts as a reminder that when engaged in these internal deliberations the possible global implications should not be neglected. An example of this is illustrated by the difficulties in reconciling strongly held bioethical positions with the practical needs of the criminal justice system when determining sample retention policy. There appears to be a consensus between the Government and civil society organisations about no longer retaining samples. The consequences of this will not necessarily just be, as police and prosecutors have indicated, missed investigative opportunities; it may also result in incorrect matches being identified. Limited data is available about the conversion of SGM personal profiles by using the SGM+ multiplex: that is an increase in maximum discriminating power from an estimate of about one in 50 million to something in the order of one in one billion. Of the 2,000 samples that were reanalysed in 2003/04, 19% were found to be invalid when the retained sample was reanalysed, but it was estimated by the NDNAD management team that the adventitious match rate could have been as high as 26%.¹⁸⁴

¹⁸³ Wilson, T. (2009), 'Forensic Science and the Internationalisation of Policing' in Fraser, J. G. and Williams, R. (eds.) *Handbook of Forensic Science* (Cullompton: Willan Publishing), pp. 493-500.

¹⁸⁴ NDNAD Annual Report for 2003/4 pp. 16 and 19.

5 Governance & Accountability

- 5.1. The arrangements for the governance of forensic bioinformation collections in the UK are under unprecedented critical scrutiny. Recent years have seen significant changes in governance arrangements, especially of the NDNAD, but there remain concerns that the present governance arrangements may be inadequate for securing confidence in the ways in which such sensitive information is collected and deployed by the police.

- 5.2. The requirements for 'good' (effective and ethical) governance remain poorly understood in the context of forensic bioinformation, yet it is essential that consistent management, cohesive policies and robust processes can be established and evidenced. This includes the future 'steering' of forensic bioinformation policies as well as the mechanisms and consequences of their current delivery. The adequacy of transparency and accountability mechanisms, including the relationship between these matters and counter-terrorism policy need examination. Further consideration needs also to be given to questions of integrity, including the setting and monitoring of quality standards and data protection and security measures. Further, there is a need for explicit deliberation about the positioning of forensic bioinformation within wider networks of personal information gathering undertaken by both State and non-State agencies.

- 5.3. There are concerns that governance arrangements of forensic bioinformation collections in the UK may be inadequate and lessons available from other bioinformation and biometric data collections in the UK and elsewhere are not being heeded. This is not because medical biobank governance is always exemplary; in fact the law governing biobanks in England and Wales has been found to be "highly complex, confusing, uncoordinated, and inadequate",¹⁸⁵ leading to the conclusion in 2007 that "there is no clear, appropriate, proportionate or effective framework for governing genetic databases, however reasonably defined, in England and Wales at the present time."¹⁸⁶ Recent analysis of the governance of biobanks within medical research,¹⁸⁷ has found regulatory structures to be "... outmoded and seriously deficient" with a governance patchwork which is "duplicative yet incomplete."¹⁸⁸

¹⁸⁵ Gibbons, S. J. Kaye, A. Smart, C. Heeney & M. Parker. (2007) 'Governing Genetic Databases: Facing Research Regulation and Practice', *Journal of Law and Society* 34 (2) pp163-189. p.171.

¹⁸⁶ *ibid.* p.188.

¹⁸⁷ E.g. ELSAGEN at www.elsgen.net; Ethox Centre 'Governing Genetic Databases' project at <http://www.ethox.org.uk/research/research-archive/governing-genetic-databases>; ESRC Genomics Forum at : <http://www.genomicsforum.ac.uk/>

¹⁸⁸ Gibbons, S. 'Regulating Biobanks: A Twelve-Point Typological Tool', *Medical Law Review*, 17, (2009) pp313-346. p.314.

- 5.4. Research into biobank governance has rarely given detailed attention to forensic genetic collections,¹⁸⁹ governance of biobanks for medical purposes being seen as separate from criminal justice purposes. Yet, as has been articulated within the biobank regulation arena:
- “...where fundamental rights, values, competing interests, risks and (public) concerns are implicated, unfettered freedom is neither beneficial nor wise. In such areas, legitimacy, fairness, justice, and the statutory ‘five principals of good regulation’ arguably demand a much more focused, coherent, properly tailored, internally nuanced, yet suitably flexible and responsive regulatory regime.”¹⁹⁰
- 5.5. This idea of the distinctiveness of forensic bioinformation collections is reinforced by the Human Tissue Act, (which created the Human Tissue Authority). This Act was intended to bring oversight to collections of human tissue, yet does not cover tissue or analysis obtained by examining or testing material that may be considered to be evidence or information to further enquiries under PACE. This reflects an important and practical division of responsibility between medical regulation and the criminal justice system to ensure that, among other objectives, there is no conflict between this system of regulation and the law relating to criminal evidence. Until the passage of the Crime and Security Act 2010, the NDNAD could be described as “essentially self-regulated.”¹⁹¹ Recent conclusions concerning the regulation of biobanks may then be even more forcefully put when referring to the governance of the NDNAD: “[there is] a de facto over-dependence on informal systems, self-regulation, and ‘soft’ regulatory techniques; and a worrying legitimacy deficit.”¹⁹²
- 5.6. Research into the ‘regulatory space’ of medical biobanks has found that regulatory systems are reliant upon voluntary compliance with systems operated *by* medical professionals, *for* medical professionals, thus raising “the sceptre of ‘regulatory capture’ and the possibility that existing governance structures lack sufficient independence and neutrality.”¹⁹³ Such a regulatory structure can also exclude other stakeholders and alienate the public, which has negative impacts: “as many studies have found, public accountability is vital for bolstering public trust, confidence, support and participation.”¹⁹⁴ The possibility of ‘regulatory capture’ is a serious risk within the field of forensic bioinformation, with databases run by the police, for the police, and overseen

¹⁸⁹ However, the ESRC Genomics Forum and GENE Banc project both have considered ‘forensic’ databases as part of their research. The former has responded to the recent HGC consultation, and the latter has published a report on forensic databanks. For an account of the latter, see GENE Banc: *Genetic Bio and Data Banking: Confidentiality and Protection of data. Towards a European Harmonisation Policy*. Available at: <http://www.genebanc.eu/> .

¹⁹⁰ *op.cit.* n.188. p.346.

¹⁹¹ *op.cit.* n.185. p.178.

¹⁹² *op.cit.* n.188. p.314.

¹⁹³ Kaye, J. & S. Gibbons, ‘Mapping the Regulatory Space for Genetic Databases and Biobanks in England and Wales’ (2008) 9, *Medical Law International*, pp111-130. p.126-7.

¹⁹⁴ *ibid.* p.126-7.

largely by the police. However, the focus should remain on good governance with visible accountability and appropriate levels of external involvement, rather than demanding the police cede control of the databases altogether, as some commentators, most notably Sir Alec Jeffreys, have suggested. As ‘owners’ and ‘users’ of the databases, the police should always remain at the centre of any arrangements since:

“intelligent accountability requires more attention to good governance and fewer fantasies about total control. Good governance is possible only if institutions are allowed some margin for self-governance or a form appropriate to their particular tasks, within a framework of financial and other reporting.”¹⁹⁵

- 5.7. The government laid out ‘principles of regulation’ in the Legislative and Regulatory Reform Act 2006, s.21(a) which states that “regulatory activities should be carried out in a way which is transparent, accountable, proportionate and consistent”. This Act was intended to bring into effect the Better Regulation Commissions’ ‘five principals of good regulation’: regulation should be transparent; proportionate; accountable; consistent; and targeted only at cases in which action is needed.¹⁹⁶ However, to fully appreciate regulation, it is important to not simply focus on just legal ‘rules’ concerning an activity or process etc., or the legal powers invested in official ‘regulators’. There can be other limitations or curbs on activities that, while they are not invoking ‘law’ directly to exert control, can nonetheless often have a regulatory effect.¹⁹⁷

The current network of forensic bioinformation governance

- 5.8. There are numerous bodies, agencies and organisations that offer resources for the setting of ethical standards for collections of bio-information,¹⁹⁸ such as the Human Genome Organisation (HUGO); the Council of Europe; and the United National Educational, Scientific and Cultural Organisation (UNESCO). Most European States also have a National Ethics Council,¹⁹⁹ and while the UK does not have such an entity, both the Nuffield Council on Bioethics, and the Human Genetics Commission have reported on forensic bioinformation.²⁰⁰ Many international organisations have outlined ‘principles’ of governance for genetic collections (mostly bio-banks for medical research purposes). According to Capron *et.al*, these have “...certain common assumptions,

¹⁹⁵ O’Neill, Onora, ‘The Reith Lectures 2002 – A Question of Trust.’ Lecture Three, available at: www.bbc.co.uk/radio4/reith2002 .

¹⁹⁶ Better Regulation Task Force, *Regulation – Less is More: Reducing Burdens, Improving Outcomes: A BRTF Report to the Prime Minister* (2005) Annex B, see also the Legislative and Regulatory Reform Act 2006, ss2 and 21.

¹⁹⁷ See Baldwin, R. & Cave, M. *Understanding Regulation: Theory, Strategy and Practice*. (Oxford University Press; Oxford, 1999).

¹⁹⁸ Known variously as ‘biobanks’; ‘genetic databanks’; and/or ‘genetic databases’.

¹⁹⁹ In the US there is the National Bioethics Advisory Commission (NBAC).

²⁰⁰ Human Genetics Commission ‘*Nothing to Hide, Nothing to Fear?*’ (2009) and Nuffield Council on Bioethics ‘*The Forensic Use of Bioinformation: Ethical Issues* (2007).

numerous points of difference, and several lacunae regarding practical issues that are not fully addressed.”²⁰¹ Indeed, the same authors claim that:

“Despite the rapid proliferation of genetic and genomic databases around the world, and the associated burgeoning of national and international guidance documents suggesting various ways of governing them, consensus over the most appropriate ethical norms and legal rules is still a very long way off.”²⁰²

- 5.9. In particular, the ‘ownership’ of genetic material remains controversial for medical researchers and lawyers alike. Ethical guidance documents may “disguise the extent to which people use the term ‘ownership’ in very different, indeed, contradictory ways.”²⁰³ Within the realm of forensic bioinformation, it is usually asserted that all information is ‘owned’ by the police and inevitably, this claim to ownership has been important in the historical development of relevant governance structures. For instance, when applying to have personal information removed, it is to the Chief Constable of the force that obtained the bioinformation that one must apply, reflecting the force ‘ownership’ of the data and samples from which the data were derived. This mirrors the fact that information on both the PNC and IDENT1, ‘belongs’ to Chief police officers, and is administered on their behalf by the NPIA. Whether this concept of ownership of such large bioinformation collections continues to be appropriate was most recently questioned by the Home Affairs Select Committee, who were told that:

“DNA profiles are owned by whichever police force entered them on the database, with the Chief Constable acting as the data controller... a strength of the current system was that data were owned by the individual police forces rather than a central organisation. They felt this guaranteed that greater care was taken in the recovery and recording of DNA material and profiles.”²⁰⁴

- 5.10. This division of responsibility and implicit assumption about ownership are given statutory force through the Crime and Security Act 2010. Should there be an opportunity for more considered legislation, the ownership issue might be revisited and the hybrid arrangements in the Act - by which, chief officers of police may make deletion decisions at their discretion in the light of principles set out in the Act, but must comply with guidance issued by the NDNAD Strategy Board, might be replaced with mandatory principles set out in a single statutory code and with an independent tribunal to determine appeals.

²⁰¹ Capron *et al*, ‘Ethical Norms and the International Governance of Genetic Databases and Biobanks: Findings from an International Study.’ (2009) 19 (2) *Kennedy Institute of Ethics Journal*, 101-124, p.102.

²⁰² *ibid.*, p.101.

²⁰³ *ibid.*, p.107.

²⁰⁴ Home Affairs Committee, ‘*The National DNA Database*’ Eighth Report of 2009-2010, March 2010, HC 222-1. para. 39.

- 5.11. While there have been recent changes to the governance of the NDNAD, these have been narrowly focussed and predicated upon the need to take the NDNAD out of the Custodianship of the Forensic Science Service, (once they became a government owned company) and then out of the Home Office. In April 2007, the NPIA took responsibility for the delivery and operational oversight of the NDNAD, ensuring it is operating to set standards as well as oversight of the laboratories and suppliers in terms of delivery of service, maintenance and accreditation.²⁰⁵ The NPIA are also responsible for all IDENT1 services, overseeing the delivery (by Northrop Grumman) of NAFIS and LIVESCAN systems by the private contractor.
- 5.12. The NDNAD Strategy Board, chaired by the ACPO lead on DNA, is responsible for the overall strategic management of the NDNAD. The NPIA, as Custodian of the database, is responsible for:
- Providing the IT infrastructure;
 - Setting the requirements and monitoring the supplier laboratories;
 - Delivering the NDNAD services to police forces;
 - Ensuring the integrity of the management of the NDNAD and the data;
 - Developing the database in line with police requirements;
 - Providing management information.

The Ethics Group acts independently, while the Forensic Regulator as their sponsor, is tasked with ensuring their independence and advising the Minister on the Group's findings and recommendations.

Issues and Prospects

- 5.13. The governance of the NDNAD in many respects sets an international and national benchmark for transparency (e.g. with the amount of information now provided in the annual report and the NPIA website). Indeed, the governance arrangements for DNA have already been subject to more public deliberation than those for other police information, including IDENT1 and the Police National Computer (PNC). Nevertheless, NDNAD governance has developed piecemeal as it seeks to catch up with the UK's pioneering use of forensic DNA. The Magee Report of 2008, looking at the broader area of criminality information and public protection, pointed out that:

“there is no overarching architecture for criminality information and no individual or organisation that could reasonably be held responsible for its absence. Each of the many organisations in the public protection network has its own accountabilities but none is accountable for the whole.”²⁰⁶

²⁰⁵ NPIA Website, accessed 1 December 2009.

²⁰⁶ Sir Ian Magee, 'The Review of Criminality Information' (The Magee Report) (July 2008) Home Office, London. p.7.

- 5.14. The NPIA may have been more forward thinking with arrangements for the new Police National Database, having sought from the outset to create mechanisms to ensure its transparency. This body is also considering the governance of, and access to, the PNC, this being a recommendation of the Magee Report.²⁰⁷ Indeed, Magee's first recommendation stated that all organisations dealing with personal information needed to clarify their governance arrangements, in particular, settling: "where ownership and accountability lie."²⁰⁸
- 5.15. There are however, concerns over the membership, oversight and transparency of the workings of the NDNAD Strategy Board. Efforts of Human Genetic Commission (HGC) members to publicly record concerns had not worked as intended and their informed 'lay' presence depends upon the continued cooperation and, indeed, existence of the HGC. A case can be made for further widening lay membership in order to maximise public involvement and engagement in order to secure confidence in the transparency of the working of the Board as well as to ensure consideration of a range of public concerns.
- 5.16. In the foreword to the 2009 NDNAD Annual Report, the Chairman of the Strategy Board conceded that the governance of the NDNAD needs to be more 'broadly based' and should "recognise the individuals and organisations that can input and contribute to the effective operation of the NDNAD." To this end, he proposes extending membership of the Board to include "the DNA Ethics Group, Human Genetics Commission (HGC), NPIA, Forensic Science Regulator and representation from Northern Ireland and Scotland and the Information Commissioner Office (ICO) as an observer." Whether this is 'broadly based' remains open to question, with members of the HGC already on the Board (as 'lay' members) and the Ethics group already playing a role. Other agencies – like the Regulator and NPIA are already included within the existing networks of forensic influence. It is also important to note that the ICO representative is included as an 'observer' only. However, he also stated encouragingly that "a collaborative approach by all the relevant agencies is the most effective way to provide oversight and direction for the NDNAD."²⁰⁹
- 5.17. A comparison with the National DNA Index System (run by the FBI) may be instructive. US National and State DNA Boards include a range of police, government, academic and civil society actors on their oversight bodies. The National DNA Index System is also monitored and audited by the Department of Justice Office of the Inspector General. There would be value in further considering the composition and remit of these bodies and those which exist in other jurisdictions. The relationship between these kinds of oversight bodies,

²⁰⁷ Recommendation 24: By Spring 2009, ACPO working with NPIA and stakeholders, should clarify the governance of the PNC and develop a clear and agreed approach in the light of the issues this report identifies as to who in which organisations should have what access to the PNC." The Magee Report p.72.

²⁰⁸ Thomas, R. & M. Walport '*Data Sharing Review*' (July 2008).p.2.

²⁰⁹ All quotes from: Chairman's Introduction, NDNAD Annual Report 2007-09, p.2.

regulators, and the various technical working groups that seek to establish quality standards in the US and elsewhere is also a subject of interest and should be investigated further. What models might be found for acceptable governance frameworks in, for example, Canadian, French or Dutch DNA database legislation? Finally, Ireland is to establish a DNA database in 2010, which will be overseen by an independent oversight committee, with unrestricted access to the database. The Committee, to be chaired by a judge (or former judge) of the High Court or Circuit Court, will report annually to the Justice Minister. There are severe penalties in place (5 years imprisonment and a Euro 50,000 fine) for unlawful disclosure of data from this database, similar to laws in place in the EU and applicable in England and Wales.²¹⁰

- 5.18. As long ago as 2001, the House of Lords Science and Technology Committee called for the establishment of an independent body: “to oversee the workings of the National DNA Database, to put beyond doubt that individual’s data are being properly used and protected.”²¹¹ Similarly, in their 2002 Report *‘Inside Information’*, the Human Genetics Commission voiced concerns about oversight of the NDNAD, recommending: “at the very least, the Home Office and Association of Chief Police Officers establish an independent body, which would include lay membership, to oversee the work of the National DNA Database custodian and the profile suppliers.” They claimed that the Government had indicated it would consider this, and “conduct a review aimed at improving the security and efficiency of the National DNA Database”.²¹² The HGC repeated their call in 2009: “we recommend that an independent body be established to oversee the management and use of the NDNAD, and that this body should conduct its business in an open and transparent way to the fullest extent that the operational sensitivities of policing will allow.”²¹³
- 5.19. The consultation paper, *‘Keeping the Right People on the DNA Database’*, envisaged supplementary arrangements to the NDNAD governance structure, but the scope and timing of these were vague. The Forensic Regulator will still have no direct oversight of the NDNAD, but will be involved in establishing and enforcing relevant scientific quality standards with respect to the NDNAD and DNA profiling. The latest government proposals in response to the consultation continue to suggest minimal changes to governance structures, with few details, except for a requirement for the Home Secretary to lay the NDNAD Strategy Board’s annual report, subject to any redactions, before Parliament, and for them to take responsibility for the guidance issued to Chief Constables over removal requests. These changes also look to be limited to the governance of the NDNAD, with no explicit mention of IDENT1.

²¹⁰ ‘Gardai get new powers to collect DNA from bodies’, *The Irish Independent*, 21 December 2009.

²¹¹ House of Lords Science and Technology Select Committee, Fourth Report *‘Human Genetic Databases’* (March 2001). Para.1.27.

²¹² Human Genetics Commission, *‘Inside Information’* (May 2002, London). p.23.

²¹³ Human Genetics Commission, *‘Nothing to Hide, Nothing to Fear,’* (November 2009, London) p.7.

- 5.20. With regard to fingerprints and IDENT1, there remain significant governance questions. There is no annual report published for IDENT1, in contrast with the NDNAD. There is also no equivalent 'IDENT1 Strategy Board' that is apparent. With the demise of the National Fingerprint Board, and the absence of any replacement, the NPIA (under the guise of Forensics21) now provides oversight of fingerprint issues nationally. Arrangements for the governance of fingerprints reflect their dual purpose: the validation of identity (e.g. to expose alias use during police enquiries or after arrest); and the establishment of identity of those individuals whose fingerprints are recovered from scenes of crime. Both of these processes are managed internally within the police service.
- 5.21. The NPIA set the operating model for the use of fingerprints, and also run the Police Database Board, (which covers all police databases), where major stakeholders are represented (though there are no external lay members). The NPIA have undertaken reviews of quality and policy and made recommendations in reports submitted to Chief Officers. There has also been comparative work undertaken between forces to ensure improvement and compliance where appropriate. These reports are submitted to the Home Office who monitor the cost benefits of their subsidy for LIVESCAN units. However there is some remaining confusion over the governance of fingerprint work. Whilst there continue to be regional meetings, practitioners need guidance on quality and policy issues surrounding fingerprinting. The international exchange of fingerprints is an issue of particular significance and seems likely to require the further development of current governance arrangements.
- 5.22. Whilst there is evidence of dissatisfaction with current arrangements for the governance of forensic bioinformation, it is also difficult to see any consensus on what mechanisms are needed to assure transparency and accountability of the uses and users of forensic bioinformation. Any mechanisms have to account for commercial considerations and interests in commercial confidentiality at the same time as making publicly available as much information consistent with concerns with security and confidentiality. There is also a need for appropriate levels of consistency in policy and practice in the management of different kinds of forensic bioinformation databases.
- 5.23. The *Marper* judgment presents a major opportunity to review current arrangements. Parliament could seek to set out 'principles of governance' either for all bioinformation collections or all forensic science collections – including both DNA and fingerprints. This requires a forward-looking perspective to provide flexibility to deal with - as yet - either unanticipated futures or developments not yet validated, in the science and its application. It may be helpful to consider the relevance of Gibbons et al (2007) eight 'desiderata' for an ideal medical biobank governance framework. In this account, a framework governance structure would:

- be firmly grounded in principle and normatively justifiable;
- reflect the characteristics and address the issues identified as being important by scientists, researchers and clinicians;
- promote and facilitate valuable, lawful, and ethical genetic research;
- provide appropriate protection for individual rights and public interests;
- contain mechanisms to resolve conflicts between competing rights, values or interests;
- be straightforward, accessible, and clearly drafted;
- have coherence, clarity and internal consistency; and
- be readily adaptable to reflect future reforms, technological advancements or changing needs.²¹⁴

5.24. In addition, there is a need for an ‘ethically robust’ approach to forensic science practice, which should be the starting point of a governance structure. As Irwin comments when considering science and ‘values’:

“Although scientific knowledge does not have a moral dimension in itself, science is conducted by individuals who certainly possess morality and values and these should be applied to their work. Scientists should ‘declare’ these values, engage with the values of the public, (and in so doing become far more likely to command public support).”²¹⁵

Such an ethically robust approach to governance, which began with attentiveness to human rights principles would require identification of relevant rights and expectations – privacy, consent, transparency, accountability, proportionality, etc.

5.25. It should also be borne in mind, that while the UK has presently not ratified the European Charter of Fundamental Rights, it became law for most EU countries on 1 December 2009. This Charter includes respect for private and family life (Article 7) but also includes Article 8, the Protection of Personal Data (see Data Protection later) and Article 41, the Right to Good Administration, which states:

- Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time...
- This right includes:
 - the right of every person to be heard, before any individual measure which would affect him or her adversely is taken;
 - the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy;
 - the obligation of the administration to give reasons for its decisions.

²¹⁴ *op.cit.* n.185. p.171.

²¹⁵ Irwin, A. ‘The Politics of Talk: Coming to Terms with the ‘New’ Scientific Governance’, *Social Studies of Science*, (2006) 36 (2) 299-320, p307.

Of course this Charter remains new and ‘untested’, and there remain difficulties in specifying the operational meaning of key terms. It cannot be applied in the UK and there is no agreement on whether this should be a consideration, or whether governance would be better shaped by reference to existing human rights protections.

- 5.26. ‘Principles’ need to be built into legislation (though readiness to rhetorically evoke such principles is often not matched by rigorous attempts to define them in the context of forensic science, the justice system or even the ECtHR). At present, the incremental approach to bioinformation, with no primary legislation effectively setting out the basis of the NDNAD or IDENT1, has meant that:

“We now have multiple pieces of legislation which need to be fitted together in order to understand exactly what is going on... what is missing is independent, accountable and powerful oversight; a fundamental reappraisal of the basis of the National DNA Database; a suitable framework for its development, its management and its governance – which is not actually in law at the moment – clarity of purpose and also articulation of the values that actually underpin this, which are lost in a morass of laws...”²¹⁶

- 5.27. In ‘*Inside Information*’, the HGC started with an overarching principle of ‘respect for persons’ from which they derived a number of secondary principles, including the principles of privacy; consent; confidentiality and non-discrimination.²¹⁷ Such ‘principles’ could then include (*inter alia*):

- consent (for victims, witnesses and volunteers), or when the law requires from suspects or convicted offenders;
- proportionality (recognised as particularly difficult to define in legislation);
- transparency (public confidence/ trust);
- accountability;
- inclusiveness (including independent lay membership of governing bodies).

- 5.28. There may be alternative or additional principles that need to be considered, and the changing conceptions of issues such as ‘privacy’ in the 21st century also need to be taken into account. How are such principles best incorporated into legislation (i.e. in relatively inflexible primary legislation, in more easily amended secondary legislation or to be interpreted and developed as a ‘living document’)? Should measures for ensuring conformity of practice and governance in line with such principles only take place at a national level when police forces are organised locally?

²¹⁶ Prof. Graeme Laurie, Evidence to the House of Lords Select Committee on the Constitution, ‘*Surveillance: Citizens and the State*’, 2nd Report of Session 2008-09, (TSO, London). para. 209.

²¹⁷ Human Genetics Commission, ‘*Inside Information*’ (May 2002), p.14.

- 5.29. Instead of a fragmented and disjointed legislative and jurisprudential framework, there is a need for a statutory basis for biometric governance which would be based upon these fundamental principles, and attentive to human rights and ethical considerations. This could take the form of primary legislation with extensive powers to modify the details of the scheme in line with the evolution of science and practice via secondary legislation. However, whilst some argue for a single piece of legislation providing the framework for the governance of all collections of forensic bioinformation, others believe that greater consideration has to be given to the intended uses of such information prior to constructing an appropriate legislative framework.
- 5.30. Any system of governance has to be capable of distinguishing between different objects of interest as well as the differing uses to which the information can be put. Whilst one-to-one identification may seem the underlying ambition of profile comparison and fingerprint matching, the additional uses of DNA samples and profiles (e.g. for familial searching and for ethnic inferencing) may create special problems that need to be separately addressed in any regulatory framework or governance arrangements. A governance strategy also needs to address issues arising from the regulation of a mixed economy within forensic science.
- 5.31. It can be argued that decisions concerning the content and use of databases and their regulation are inextricably linked. It is useful then to think first about DNA and fingerprint practice – the collection from whom, comparison with what records for what investigative purposes, etc. – and only then decide on the appropriate framework within which regulation should be located. The Human Genetics Commission have called for a ‘definition of purpose’ and stress that there is a need for a clear purpose will then precipitate clarity on other questions such as retention, governance etc. Legislation and operational practice can then follow, for example, legislation should clearly delineate ‘boundaries’ for the use and protection of bioinformation/ forensic science e.g. if used for ‘counter-terrorism’ purposes.
- 5.32. So before legislation is drafted, a number of questions need to be addressed in order to ensure clarity, and that the legislation is providing the powers and governance that are necessary for ‘success’. Such questions would include:
- What are the range of uses to be made of the data (bioinformation) and what safeguards are required to protect its integrity and keep it secure?
 - What is it that makes data ‘sensitive’ when the state/ police hold it?
 - Is bioinformation more ‘sensitive’ than any other police information?
 - Is DNA data more ‘sensitive’ than fingerprint data?

- Can requirements for good governance of bioinformation stand apart from the requirements for good governance of forensic science in general?
 - Is any police information ‘more’ sensitive than other types of public protection information (i.e. immigration; vetting and barring information etc.) – in which case do we need a ‘public protection information’ governance framework?
 - Are new issues raised by:
 - the increasing effort to ‘join-up’ information databases;
 - the needs of counter-terrorism;
 - the increasing use of such data collections for the identification of bodies, especially in Disaster Victim Identification work?
- 5.33. Greater consideration of the type of information, and the uses to which it can be put are essential for shaping any new governance structure for this domain of public life. As Magee points out: “effective governance requires an appropriate balance of ownership, process and control... the key requirement is for a governance mechanism that is aligned to the purpose it serves.”²¹⁸ There may be a need for multiple frameworks of governance, particularly if the new governance structures are intended to have broad application – for example, to all forensic bioinformation types, to all forensic science, or even all personal information managed by the police, or information for public protection.
- 5.34. If bioinformation were to be regarded as primarily a source of information for the police, then it might come to be managed under MOPI (Code of Practice on the Management of Police Information, 2005).²¹⁹ This Code of Practice was introduced in direct response to criticism in the Bichard Report about the handling of information concerning Ian Huntley prior to the murder of two young girls. This would clearly have an impact on the overall governance structure, and integration of different forms of information and management of MOPI, together with the ultimate scrutiny of police information by the Information Commissioner’s Office.
- 5.35. Magee has recently called for the creation of a ‘public protection network’ which would encompass all agencies that have a public protection and crime prevention remit, and hold and process personal data to fulfil that role.²²⁰ This

²¹⁸ Magee ‘*The Review of Criminality Information*’ (Magee Report, July 2008) Home Office, London. p.23

²¹⁹ MOPI is described as ‘a statutory code’. It has been promulgated by the Home Secretary under the Police Acts of 1996 and 1997 (as amended by the Police Reform Act 2002). This legislation sets out the scope of the code and requires that any such code be laid before Parliament after promulgation and may contain requirements about consultation, but not that the code itself requires consent or may be annulled by Parliament as if it were secondary legislation. ‘Chief Officers [of police] are required under the Act to “have regard” to any such codes’ (Forensic Science Regulator (2008) Manual of Regulation - Part One: Policy and Principles, p19 (London, Home Office).

²²⁰ This would then include the police and all associated departments under the police umbrella (such as SOCA/ counter terrorism groups etc.); ‘barring and vetting’ agencies such as the Criminal Records Bureau; immigration agencies including the UK Borders Agency, and the Independent Safeguarding Authority etc..

network would then include all relevant agencies and their data, although the size and complexity of the network would create particular challenges:

“On the one hand we need agile, empowered organisations that can respond swiftly to specific and local needs. On the other we need mechanisms that will ensure the safe and appropriate capture, sharing and use of criminality information between these organisations – including between nations – and which will command public confidence.”²²¹

Magee outlines those details requiring explicit agreement and recording across the protection network that would make clear ownership and decision making rights, including:

- “Capture: what information do we seek, for what purpose, and how do we gather it?
- Storage: where do we store it, for how long, and under what security?
- Access: how can it be accessed, who has the right to do so, and do they have the ability to change the information?
- Sharing: what interconnections should and do exist between repositories of information, what is the nature of those connections? E.g. does one master copy of the record exist, or is the information broadcast to multiple repositories? How rapidly is information available to those who need it?
- Analysis: is information available in a format suitable for its intended use and when it is needed?
- Action: do decision-makers act on the basis of the information available, and do their actions result in successful outcomes?
- Management: do managers understand the performance of the PPN, the contribution of this information to this and are they able to communicate it to staff?”²²²

The challenge of governing a large and dispersed group of agencies and individuals would be met by: “focused, independent and long-running accountability...”.²²³ This would not be a task for the Information Commissioner alone as decisions about the effective use of the data for public protection would be beyond the (present) scope of his role.

²²¹ *op.cit.* n.218. p.23.

²²² *op.cit.* n.218. p.28.

²²³ *op.cit.* n.218. p.33.

Scientific and Organisational Integrity

Quality Standards

- 5.36. Much effort in recent years has gone into establishing and sustaining consistent quality standards in DNA profiling. The strong emphasis on quality assurance for this technology contrasts with other forensic disciplines. The role of the UK Forensic Regulator, with the responsibility of overseeing the quality of all forensic science, was created in 2007. The Regulator's Manual (still in draft form and requiring detailed appendices) sets out requirements for all forensic science services, in order to maximise the effectiveness of the criminal justice system and maintain public confidence in the quality and reliability of the forensic science provided to police forces and others. To do this, the Regulator establishes and monitors quality standards and ensures accreditation of suppliers of forensic services, including quality standards which apply to national forensic science intelligence databases. The NDNAD is mentioned specifically in this regard, although IDENT1 is not.²²⁴ Section 12 of the Regulator's Manual states that the Regulator has a role in overseeing quality standards applicable to national forensic science intelligence databases. The December 2009 Report from the Regulator states that he is to release quality standards for the NDNAD and National Ballistics Intelligence Service databases for consultation in early 2010.
- 5.37. The Interim Regulator undertook two reviews of the application of forensic DNA technology during the first year of the Regulator's office. However, neither have been made public because of 'commercial confidentiality'. A third review, of LCN DNA was undertaken by the new Regulator during 2008 and was published on the Home Office website.²²⁵ In 2010, the Regulator is undertaking reviews of familial searching as well as setting standards for new common frequency databases to be used in future DNA profiling systems.²²⁶
- 5.38. The Forensic Regulator oversees accreditation (via UKAS) of all laboratories that supply DNA profiling services to the police. Scenes of crime examination are included within his accreditation schedule. However there remain questions over whether quality regulation reforms are being applied equally to all aspects of bioinformation collection, retention, and usage. The regulator does not for example, play a similar role in accrediting fingerprint bureaux, nor police custody suites, where fingerprints and DNA samples from suspects are acquired. Seven suppliers currently provide profiles to the NDNAD,²²⁷ each of whom must be accredited to ISO17025 & Custodian Standards for accreditation

²²⁴ The Forensic Science Regulator, Business Plan 2008/09 – 2010/2011, para 3. available at http://police.homeoffice.gov.uk/publications/operational-policing/Forensic_Science_Regulator_3.html .

²²⁵ *ibid.*, para 11.

²²⁶ The Forensic Regulator, Report, (December 2009), p.9.

²²⁷ The FSS Ltd; LGC Ltd; Orchid Cellmark; SPSA (Scottish laboratories); FSNI (Northern Ireland); FDS (Forensic DNA Services); Eurofins (EFS & Medigenomix) with another coming on stream in 2009.

(LAB 32) and approved by the National DNA Database Strategy Board. They need to demonstrate that they have in place anti-contamination measures (including elimination databases of staff and manufacturers, and un-sourced contaminant profiles). Their profiles must meet the minimum load criteria and meet duplication requirements. They must also take part in closed proficiency testing and validate their process and system changes.

- 5.39. On the one hand, the introduction of a regulator was presented as creating a generic standard for forensic science providers in the UK – based on ISO standards and ‘a light touch’ in steering providers, but there remain concerns about perceived lack of ‘teeth’ and gaps in regulation with a fear that accreditation may prove to be superficial. Civil remedies for breaches of regulatory standards may be too little, too late and cannot provide an answer to mistakes already made within the criminal process. It is a matter of regret that the UK, as a world leader in privatising its forensic science providers within an adversarial system, had not properly set-up a regulator system before the introduction of a mixed economy. The emerging shape of the forensic science marketplace remains difficult to discern. The work of regulating the provision of goods and services within this marketplace has only recently begun and deserves careful examination.
- 5.40. The December 2009 Regulator’s Report states that the Home Office has now established a ‘Forensic Science Strategy Group’, including the Regulator and Chaired by a Home Office senior civil servant, which will meet monthly. This group is intended to supplement the work of the Regulator, whose remit does not extend to the broad range of risks to the supply and use of forensic science, although the Regulator will also be forming an additional sub-group to ‘identify and manage this broader array of risks’.²²⁸ The Regulator is also extending his work to provide guidance on the interpretation and presentation of forensic evidence to prosecuting authorities and courts, with a new specialist group established for this purpose. There are clear moves then to extend the Regulator’s work into areas that he had previously been reluctant to enter. There will also be interplay between the Home Office forensic science strategy group and the work of the Regulator. The constitution and remit of the Home Office group is as yet unknown.
- 5.41. The requirement to have quality standards and accreditation has now become part of an EU Council framework decision (15905/09). With international exchange increasing, it is vital that quality standards in forensic science can be assured across Europe: “The adoption of common quality standards for forensic science across Europe has become ever more important as the international exchange of DNA profiles offers greater potential to increase public safety in a

²²⁸ The Forensic Regulator, Report, (December 2009), p.3.

significantly more mobile society.”²²⁹ Now, ‘laboratory activities’ carried out by forensic science providers must be accredited so that public authorities in each country can recognise results generated by a laboratory in another EU country. The national accreditation body of each member state will then ensure compliance with the relevant international ISO standard. However, there may still remain gaps in oversight with regard to forensic bioinformation, with fingerprint bureaux not included under ‘laboratories’, only fingerprint development laboratories. This distinction permits police fingerprint bureaux to continue operating without requiring ISO accreditation.

Data Protection and Security

- 5.42. Concerns over the use of personal information are not new, though they may be attracting greater attention. The European Commission found that in Europe:

“public unease about the use of personal information is widespread and has remained consistent for almost twenty years. Some 64% of EU respondents – and as many as 77% of UK respondents – expressed concerns about whether organisations holding their personal data handle it appropriately.”²³⁰

The security of data, particularly personal data, has gained prominence however, since a series of high profile losses of sensitive information, mostly by public sector agencies, as highlighted in the Thomas & Walport report:

“Repeated losses of sensitive personal information in both the public and private sectors demonstrate the weakness of many organisations in managing how data are shared. The advent of large computer databases has allowed the loss of massive datasets in ways that were simply impossible with paper records.”²³¹

- 5.43. The Trustguide Report (2006) found a feeling of ‘vulnerability’, where people reported a lack of ‘control’ over the data collected about them, and this was most acutely felt around their ‘identity’:

“Technology creates many new challenges and causes us to redefine that which we may have taken for granted in the physical world and one field where this is most apparent is the creation and protection of one of our most valued and most used attributes – our identity. ... Attendees reported that as more data is gathered and stored electronically, particularly in centrally controlled databases, they feel more vulnerable. Most of this vulnerability is focused on a lack of control over who is collecting their

²²⁹ Foreword, CC Neyroud, NDNAD Annual Report 2007-09, p.4.

²³⁰ Eurobarometer: Data Protection in the European Union – Citizens Perceptions (February 2008). – available at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm .

²³¹ Thomas, R. & M. Walport ‘Data Sharing Review’ (July 2008).p.i .

data, who might have access to it, how their data may be used now or in the future and the potential for function creep..”²³²

- 5.44. The Coleman Report (2008) examined the risk of fraud, accidents (including loss of data); cyber-attacks and threats etc. to government information holdings.²³³ There is clear public concern over the processing and sharing of data by government agencies as well as how securely they hold them. Victim Support state that they believe the public are unconvinced that DNA data can be stored securely: “...the Government should take steps to assure the public that data on the [DNA] database is secure, and that the database contains only that information which is necessary to adequately protect the public.”²³⁴
- 5.45. The Information Commissioner dealt with 94 breaches of the Data Protection Act in the five months preceding April 2008 alone, indicating that these are far from isolated incidents. Control of data becomes a greater issue with increases in the amount of protected data and the number of users of the data. Many breaches, some which may occur daily, can be relatively insignificant, with little impact and no sanctions necessary. However, some breaches have been significant, with serious implications and high profile media attention has led to a plethora of reports, inquiries, and reviews, including the ‘*Data Handling Review*’ (Hannigan Report), which culminated in a new Security Policy Framework which provides the guidance on security and risk management for all government (and associated) bodies, including the police. The SPF contains 70 minimum security requirements that must be adhered to by all government bodies and agencies, including suppliers of services.
- 5.46. The NDNAD Annual Report (2007 – 2009) states that “many of the minimum standards...were already met or exceeded by the security measures in place for the NDNAD.”²³⁵ However, a comprehensive security review resulted in new working practices and increased monitoring of activity, leading to improvements including: reinforced security training for staff; revised incident management scheme which includes reporting to the ICO; additional specific measures to protect personal information; stricter controls and measures for the use of removable media; security clauses in all contracts with external providers; increased audit and management accountability. The NDNAD has also been brought within the NPIA main data centre and the use of fax machines has been phased out, with all communications now undertaken via secure government email with strict audits and controls and overlying encryption when required. The NDNAD Annual Report goes on to affirm that:

²³² Lacohee, H., S. Crane, and A. Phippen, ‘*Trustguide: Final Report*’, (Trustguide, October 2006), p 84.

²³³ *Protecting Government Information* – Independent Review of Government Information Assurance (The Coleman Report), June 2008, Chapter 3.

²³⁴ Victim Support, ‘*Response to Keeping the Right People on the DNA Database*’ (July 2009), p.1

²³⁵ NDNAD Annual Report 2007-2009, p.36.

“Security continues to be given the highest priority within the NDNAD Delivery Unit and by the NPIA senior management who are committed to a process of continuous improvement for the NDNAD and to an ongoing programme of technical and procedural compliance audits to ensure that the high standards which have been set are embedded and being implemented within day operational practices by all operational staff.”²³⁶

- 5.47. The generous accessibility of the PNC, in addition to the practice of sending demographic details attached to DNA samples to laboratories for analysis, demonstrate that there may still be ample opportunity for improper access or lapses in security. The Crown Prosecution Service, in the spotlight for serious data losses, have recently reviewed and altered policies on their security, including the use of portable media and encryption. Work on further reducing risk and strengthening “information risk governance, covering both personal data and other sensitive information” is ongoing.²³⁷ Other law enforcement agencies that receive or use forensic bioinformation may also be forced to undergo such reviews to ensure their data security.
- 5.48. Relevant to discussion of data governance is consideration of what kind of data protection laws exist in relation to DNA profiles and fingerprints generated for criminal justice purposes only. In some jurisdictions, data protection regimes differentiate between the collection and retention of personal data for criminal justice and other purposes, but however these regimes operate it is necessary to understand their application to DNA profiles and to fingerprints before there can be agreement on a governance model for forensic bioinformation.
- 5.49. The EU Directive 95/46/EC on Data Protection,²³⁸ which is currently under review, came into force in October 1998, being given effect in domestic law by the Data Protection Act 1998. The EU directive focuses on the protection of individuals with regard to the processing of personal data and the free movement of such data and applies to DNA data unless specific DNA legislation determines otherwise. Article 6 of the EU Directive states that personal data must be: adequate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed; and kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The preamble to the Directive states:

²³⁶ *ibid.*, p.37.

²³⁷ The Cabinet Office, ‘*Data Handling Procedures in Government: Final Report*’ (The Hannigan Report), June 2008, p.29.

²³⁸ See: Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, available at www.europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm .

28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified.”

Not all UK commentators feel that Section 64 of PACE is sufficiently exact to meet the requirements of this Directive.

- 5.50. The Data Protection Act 1998 is based upon eight data protection ‘principles’ derived from this EU Directive, that can be applied to the use of all personal data, including the third principle that states that data must be adequate, relevant, and not excessive in relation to the purpose for which they were obtained, while the fifth principle states that data should not be kept for longer than is necessary for the purpose(s) for which it was collected. The seventh principle states that “appropriate technical and organisational measures shall be taken against any unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”
- 5.51. In 2001, the EU established a European Data Protection Supervisor to oversee the implementation of data-protection standards within EU institutions. Regulation (EC) 45/2001 also introduced strict rules on data processing and rights for citizens to access their data. Article 20 however, permits law enforcement authorities significant exemptions from the data protection regime, including the processing of forensic data. This limits the role of the EDPS with regard to forensic data, although he has been highly critical of the Prüm Treaty.
- 5.52. In the new European Charter in Fundamental Rights (which the UK has not signed), Article 8 concerns the protection of personal data, stating that:
- Everyone has the right to the protection of their personal data;
 - Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law;
 - Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified;
 - Compliance with these rules shall be subject to control by an independent authority.

5.53. It is probably the case that such requirements would be easily met by proper adherence to the Data Protection Act 1998. However, application to all data – whether for policing or other purposes – would mean that data protection would encompass the use of forensic bioinformation across the EU and could have significant implications, and may require the greater involvement of the Information Commissioner than has hitherto been the case in the UK (even though he now sits on the NDNAD Strategy Board as an ‘observer’).

5.54. The original EU Directive may also be in need of updating:

“Fuelled in part by technological, commercial and social developments since its adoption in 1995, voices in some quarters are increasingly questioning whether the Directive, and by inference the UK’s DPA, is still fit for purpose. Some are calling for the Directive to be reviewed.”²³⁹

Moves to strengthen data protection across the EU may dramatically impact upon domestic data protection. For example, the European Council Framework Decision of 24 June 2008 on the protection of personal data processed for police and judicial cooperation in criminal matters emphasises the need for time-limits for erasure and review. Yet in the UK, following the Bichard Inquiry, changes to the law including: the retention of fingerprints and DNA; the admissibility at trial of bad character evidence; obligations to provide information to the CPS and the courts, etc. resulted in ACPO reviewing their ‘weeding’ policies (removing ‘old’ convictions from the PNC). Though still maintaining the ‘step down’ system (where some old convictions are made only available to the police), they moved to a complete system of retention whereby no convictions are deleted or ‘weeded’ from the PNC except in exceptional circumstances (i.e. if the conviction was wrongly obtained).²⁴⁰

5.55. The ‘Five Chief Constables’ case²⁴¹ was prompted by the disclosure of old convictions relating to five individuals, to potential employers as the ‘stepping down’ procedure did not prevent disclosure in such circumstances. The Information Tribunal ruled that this policy of permanent retention of all convictions was unlawful under the Data Protection Act 1998, and this was appealed by five Chief Constables in the Supreme Court. The Appeal concerned whether two of the principles of the DPA were being complied with: DPP 3 which states that excessive data must not be retained and DPP 5, that data must not be retained longer than necessary. The police used the ability to re-open ‘cold cases’ with DNA advances as just one justification for permanent retention of conviction data.

²³⁹ Thomas, R. & M. Walport ‘Data Sharing Review’ (July 2008).p.22.

²⁴⁰ The areas of bad character evidence, the CPS and courts’ requirements were covered in the EU Framework decision 2009/315/JHA and updated provisions are in the Coroners and Justice Act 2009.

²⁴¹ *Chief Constables of Humberside Police; Staffordshire Police, Northumbria Police, West Midlands Police, and Greater Manchester Police, and the Information Commissioner, and the Secretary of State for the Home Department* [2009] EWCA CA Civ 1079.

- 5.56. Lord Justice Waller stated that compliance with the first Data Protection Principle (that data must be processed fairly and lawfully) did not require constraints be placed upon the purposes for which data is retained (as long as they are lawful), but that it is important “that people know what the data is being retained for and so that the Information Commissioner and data subjects can test the principles under the DPA by reference to the purposes identified.”²⁴² Further, Lord Justice Carnwath ruled that with respect to the PNC, Article 8 (5) of the EU Directive recognised the importance of maintaining a ‘complete register of criminal convictions’ provided that it is “under the control of official authority” and there existed suitable safeguards provided under national law, thus: “The power to maintain “a complete register”, to my mind, logically encompasses power to maintain records of all convictions, without regard, for example, to age or relative seriousness.”²⁴³ It was pointed out that with regard to the *S & Marper* ruling, “the nature of the information was quite different.” and the case “is no authority for the proposition that a record of the mere fact of a conviction engages Article 8.”²⁴⁴
- 5.57. Questions of the effectiveness of data protection legislation with regard to forensic data then raise uncertainties about the powers of Data Protection Commission staff. In the ‘Five Chief Constables’ case, it was ruled that the ICO was meant simply to ‘review’ the police policy on data retention, not replace the police judgment with his own. While the ICO has recently been given the power to impose financial penalties, questions remain surrounding the proper use and extent of his powers. There is also a need for better understanding of how these powers are actually exercised in the course of routine and exceptional uses of forensic bioinformation. The Dutch Data Protection Authority has the right to audit the DNA database and exercises this right regularly. The ICO has been involved in discussions with ACPO in respect of some uses of the NDNAD (in particular familial searching). The resulting ‘Memorandum of Understanding’ details safeguards that have been agreed and the ICO has approved the use of familial searching when: “restricted to the most serious cases and intrusion into the private lives of individuals is minimised.”²⁴⁵ The precise nature of relevant safeguards are unknown, however as the MOU is not a public document.
- 5.58. To date, the ICO has had limited involvement with the NDNAD, prior to the commencement of his observer role on the Strategy Board. It is unclear whether the ICO has any involvement or oversight of other forensic intelligence databases. However, the Information Commissioner’s response to the Government consultation expressed surprise at the lack of mention of the DPA, given that the issue centred upon the fair and lawful use of personal data. As he and others point out, the obtaining and retention of forensic bioinformation clearly engages the First Principle of the DPA, while the indefinite retention

²⁴² *ibid.*, para.31.

²⁴³ *ibid.*, para.72.

²⁴⁴ *op.cit.* n.241. para.80.

²⁴⁵ *op.cit.* n.218. p.89

engages the requirements of the Third and Fifth Principles:

“The fifth Data Protection Principle requires that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. For DNA profiles on those who have not been convicted the retention period needs to be necessary for the purpose of policing. ‘Necessary’ in this context, means more than useful.”²⁴⁶

Yet no attempt was made throughout the consultation document representing the Government response to *Marper*, to “address any of the obvious data protection compliance issues.”²⁴⁷

Scientific Research and Technological Development

5.59. The use of genetic collections for research is well established in the medical field, and there is a wealth of material available on how research is to be approved etc., though the network of ethical committees are often labyrinthine. The House of Lords Science and Technology Select Committee affirmed the need for strong oversight of research using genetic databases in 2001, or the promise of genetic research would not be realised:

“...robust systems with strong oversight mechanisms were needed to ensure that research on human genetic databases was carried out to the highest ethical standards, in both private and public sectors....”²⁴⁸

“arrangements for the handling and analysis of personal data held in human genetic databases should be carried out to the highest ethical standards, with proper attention to the rights of the individual to privacy and confidentiality of their personal medical and other data. It is essential that there is high public confidence in this activity, otherwise some or many of the benefits to be gained from the advances in genetics will not be realised.”²⁴⁹

5.60. The maintenance of high scientific standards is dependent largely upon proper forensic research. However, the role of Research Councils and major charities in funding forensic science research remains unclear. Efforts by the NPIA, the Association of Chief Police Officers (ACPO) and others to encourage university research should be supported in the hope that the wider scientific community becomes willing to participate in this work. Such university research will require

²⁴⁶ Information Commissioners Office, *Response to ‘Keeping the Right People on the DNA Database’*, August 2009, p.7.

²⁴⁷ *ibid.*, p.4.

²⁴⁸ House of Lords Science and Technology Select Committee, Fourth Report ‘*Human Genetic Databases*’ (March 2001). Para.7.34.

²⁴⁹ *ibid.*, para.7.46.

support in terms of access to data. It may be useful to consider what kind of partnerships may be possible between NPIA and other actors in order to secure research and development funds. The UK forensic field is not proactive in assessing risks and measuring 'quality' however. Moreover, unlike the USA's National Institute of Standards and Technology (NIST), there is no longer a government/publicly funded organisation in the UK to set relevant standards for the forensic community.

5.61. Arrangements for the use of the NDNAD or cellular materials retained by providers for research have become more transparent in recent years. The Ethics Group made it one of their main priorities to prepare proposals for the Strategy Board that would create a clear and effective governance framework for this. At present, those making research requests direct these to the Custodian, who then provide the details to the Strategy Board. Each proposal is assessed on its merits and further advice sought from the Ethics Group. The NDNAD annual report states that requests are not agreed unless they have 'clear operational benefits to the police', but details in the public domain remain scant as 'commercial confidentiality limits what details can be provided about specific research proposals.'²⁵⁰ Figures are provided with a short description outlining the general purpose of the research. Since 1995, there have been 46 requests for access to samples or data with 26 have been approved, 18 have been rejected and two remain under consideration (as at 31st March 2009).²⁵¹ For further 'operational' work to be done using the NDNAD (e.g. Y-STR work) written authorisation is required from the police force ACPO officer, the CPS caseworker, as well as the Chair of the NDNAD Strategy Board.²⁵²

5.62. Despite the use of so-called 'junk DNA', as the Police Foundation have claimed, this process may be insufficient and requires clarity and transparency:

"DNA samples are an intimate window into a person's make-up and reveal a wide range of genetic information including details relating to their personal health and family relationships. The Police Foundation would welcome detailed guidelines on how the DNA will be used and assurances as to the future use of profiles or planned research as well as confirmation as to which bodies will be allowed access to the data."²⁵³

It is clear however, that the use in research of DNA profiles or retained samples by third parties is a matter of public concern. The HGC Report '*Inside Information*' reported that:

²⁵⁰ NDNAD Annual Report 2007-2009 p.41.

²⁵¹ *ibid.*, p.38.

²⁵² *ibid.*, p.42.

²⁵³ Police Foundation response to '*Keeping the Right People on the DNA Database*', (2009), p.4.

“Two thirds of those in our People’s Panel survey felt any access was inappropriate. Others felt that if there is to be any access.... for research purposes then this should (a) only by for the purpose of crime detection and prevention and (b) the normal conventions of medical research should apply with regard to informed consent and confidentiality.”²⁵⁴

- 5.63. Research with actual or potential forensic science applications may often be carried out ‘on the back of’ more generic scientific research conducted in universities and elsewhere. However, following the changed status of the Forensic Science Service, it is not clear which bodies may have a role in searching for or disseminating the results of scientific work with potential forensic applications. There remain significant and distinctive problems surrounding IPR in forensic science research, and ways need to be found of balancing the need for commercial confidentiality with the interests of the court in transparent and reproducible scientific work.

Public Confidence and Trust

- 5.64. A key criterion for effective policing is public consent. As Flanagan stated in his 2008 review of policing:

“Policing is far too important to be left to the police alone. It is a public service and one that can only be effectively carried out with the support and consent of the public. Using and developing this engagement with the public is one of the most important challenges in modern policing and it is a challenge that must be met at all levels.”²⁵⁵

Indeed, Flanagan states that the public: “must always be the single most important aspect of policing” as it is only through engagement with the public can the police understand their priorities, and be accountable.²⁵⁶ Public opinion is therefore an important aspect of policing by consent, but more widely, is vital to any policy decision-making within a representative parliamentary democracy.

- 5.65. For public consent to policing to be maintained, they must have confidence in the police and their governance. Public confidence features prominently in Public Service Agreement 24 concerning the effectiveness, transparency and responsiveness of the criminal justice system as a whole. Openness and transparency are crucial to the gaining and maintenance of public confidence and trust in the operation of all organisations. It is crucial not just for the operation of the criminal justice system, but for government as a whole, that

²⁵⁴ Human Genetics Commission, ‘*Inside Information*’, para.9.50.

²⁵⁵ Flanagan Report ‘*The Review of Policing – Final Report*’ (February 2008) Home Office, p.5 available at www.police.homeoffice.gov.uk/publications .

²⁵⁶ *ibid.*, p.7.

there is trust in public institutions, indeed, “Trust is the basis for human rights and democracy.”²⁵⁷

5.66. As has been stated on many occasions, the use of forensic bioinformation during investigations and prosecutions requires the confidence of the public for it to be effective in securing convictions. The public may also expect the government to exercise their duty of care and utilise technologies available to them in order to protect the public.²⁵⁸ However, the public also need to trust that government will use technologies wisely and not overreach their powers. With the storing of sensitive data, the public need to have confidence that the databases are secure and being used legitimately. As the Fraser Report states: “The DNA database stores private genetic information and continued public confidence in the legitimate use and adequate safeguarding of this information relies on accountability and transparency of information.”²⁵⁹

5.67. The House of Lords Select Committee on the Constitution previously claimed that policy-making in the area of surveillance has not been up to standard, with too few details and a lack of specificity in legislative Bills, meaning that Parliament was unable to effectively scrutinise proposals.²⁶⁰ The Committee also stated that: “The openness of organisations, both about their personal information and surveillance plans and practices, and about ways in which the public can be more effectively involved in understanding and shaping them, is important.”²⁶¹ The Committee argue that:

“If trust in relationships between the citizen and the state is to be maintained, public understanding of surveillance and the way in which personal data are processed must involve organisational transparency, starting at an early stage in the Government’s policy proposals.”²⁶²

5.68. The Thomas-Walport Report also portrayed transparency as a prerequisite for public trust, emphasising that public bodies must provide clearer and better information to the public about data sharing.²⁶³ That standard-setting bodies must operate in an open and transparent way is a ‘basic requirement for public trust’.²⁶⁴ The Royal Commission on Environmental Pollution considered that ‘transparent’ meant: “there must be full publicity for their existence, their terms

²⁵⁷ O’Neill, Onora, ‘The Reith Lectures 2002 – A Question of Trust.’ Lecture Two, available at: www.bbc.co.uk/radio4/reith2002

²⁵⁸ Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance* (RAE, London, March 2007) p.44.

²⁵⁹ Fraser, J. (2008) *Acquisition and Retention of DNA and Fingerprint Data in Scotland* p.14 as published in September 2008 at www.scotland.gov.uk/Consultations/Current .

²⁶⁰ House of Lords Select Committee on the Constitution, ‘*Surveillance: Citizens and the State*’, 2nd Report of Session 2008-09, February 2009, The Stationary Office, London. para. 357.

²⁶¹ *ibid.*, para.433.

²⁶² *ibid.*, para.434.

²⁶³ Thomas, R. & M. Walport ‘*Data Sharing Review*’ (July 2008). para 8.14.

²⁶⁴ Royal Commission on Environmental Pollution, (1998), ‘*Setting Environmental Standards*’, 21st Report, (London, The Stationery Office).

of reference, the decisions they take and the reasons for them...”, while ‘openness meant that: “there must be adequate opportunities for those outside an institution...to contribute fully to the decision-making procedure.”²⁶⁵ ‘Transparency’ however can be a catch-all term that can mislead, with the Thomas-Walport Report leading to provisions in the 2009 Coroners and Justice Bill, later dropped, that included almost carte-blanche data-sharing between government departments and bodies, a move that was widely rejected.

5.69. The Government has made a commitment to enhanced transparency, outlining ‘key principles’ to which they will give due regard when reviewing policy:

- Are robust safeguards in place to protect information and individual liberties?
- Are our plans and actions proportionate to the damage and the threat they are seeking to prevent?
- Are we being as transparent as possible? Are citizens being given the right amount of choice?²⁶⁶

All government departments are required to publish ‘Information Charters’ which outline the information they keep, how it is used and contained, with a presumption of openness. However, “there will always be some information and some uses of it (e.g. in the area of national security and law enforcement arenas) where transparency must rightly be limited...”²⁶⁷ The government has however, demonstrated this commitment to openness and transparency in other areas, for example in 2008 the National Security Strategy was published,²⁶⁸ committing government departments to publicly available standards, and in 2009, the new Security Policy Framework, which sets out universal mandatory standards for security of information in government, has largely been placed in the public domain for the first time; “allowing greater access, increasing awareness, transparency, and sharing good practice.”²⁶⁹

5.70. However, the development of IDENT1 and the establishment of the NDNAD have until recently been considered operational policing matters and decisions have been taken internally, without public consultation or external involvement. A similar situation as has occurred in other countries setting up their DNA databases, resulting in difficulties with public confidence:

²⁶⁵ *ibid.*, p.124.

²⁶⁶ Government Response to the House of Lords Select Committee on the Constitution’s Report: ‘*Surveillance: Citizens and the State*’, 13 May 2009, Cm7616, The Stationery Office, London. p.1.

²⁶⁷ The Cabinet Office, ‘Data Handling Procedures in Government: Final Report’. June 2008, p.23.

²⁶⁸ Cabinet Office Homepage, ‘*Understanding the Security Policy Framework*’ available at:

<http://www.cabinetoffice.gov.uk/spf/faqs.aspx> accessed on 23 December 2009.

²⁶⁹ Sir Gus O’Donnell, ‘Foreword’ in ‘*HMG Security Policy Framework*’ (October 2009), p.5

“Clearly there has been little opportunity for civic engagement and biological citizenship with respect to the establishment and operation of forensic DNA databases in Australia... there has been a technocratic policy approach....A strong companion of technocratic systems in public distrust.”²⁷⁰

- 5.71. Rose & Novas’s concept of ‘biological citizenship’,²⁷¹ stresses the importance of democratic decision-making with regard to bioethical issues. In recent years the Government have at least espoused a new more ‘open’ form of decision making, with the public engaged in science policymaking. Tony Blair claimed in 2002 that: “the benefits of science will only be exploited through a renewed contract between science and society, based on a proper understanding of what science is trying to achieve.”²⁷² Indeed, in 2000, the House of Lords Select Committee on Science and Technology recommended that “direct dialogue with the public should move from being an optional add-on to science based policy-making and to the activities of research organisations and learned institutions, and should become a normal and integral part of the process.”²⁷³
- 5.72. However, a commitment to social consensus on science policymaking assumes the location of an elusive ‘public’ with a homogenous ‘public opinion’.²⁷⁴ The House of Lords Select Committee on the Constitution have previously stated that: “Assertions about what ‘the public’ feel or want concerning surveillance are not conclusive, although they do often go unchallenged.”²⁷⁵ Within the realms of forensic bioinformation, this can clearly be seen to be a false expectation, as public opinion concerning forensic bioinformation varies widely. Accordingly it is legitimate to ask how seriously public engagement is taken in this area of scientific development “in particular, what is the relationship between this broad rhetoric and institutional practice?”²⁷⁶
- 5.73. It is not obvious that the consultation: “*Keeping the Right People on the DNA Database*”, seriously affected the Government’s eventual proposals. The range of responses tended to support the argument that even when the public respond negatively to developments, or disagree with policy suggestions, the more centralised control over risk management, and ‘professionalisation’ of bodies such as the police/ Forensic Regulator, to make decisions, could mean

²⁷⁰ Hindmarsh, R. (2008) ‘Australian biocivic concerns and governance of forensic DNA technologies: confronting technocracy’. *New Genetics and Society*, 27(3) 267-284, p.278.

²⁷¹ Rose, N. & C. Novas (2005) ‘Biological Citizenship’, in: A.Ong, & S.Collier (eds) *Global Assemblages: Technology, Politics and Ethics as Anthropological Problems*. Oxford, Blackwell, 439-463.

²⁷² Tony Blair, ‘Science Matters’, 10 April 2002 available at: www.number-10.uk/output/Page1715.asp .

²⁷³ House of Lords Select Committee on Science and Technology, (2000) ‘*Science and Society*’, (London, The Stationery Office), p.43.

²⁷⁴ see: Irwin, A. ‘The Politics of Talk: Coming to Terms with the ‘New’ Scientific Governance’ *Social Studies of Science*, (2006) 36 (2) 299-320, p.303.

²⁷⁵ House of Lords Select Committee on the Constitution, ‘*Surveillance: Citizens and the State*’, 2nd Report of Session 2008-09, February 2009, The Stationary Office, London. para. 399.

²⁷⁶ *op.cit.* n.274., p310.

that: “the possibilities for public challenge to the dominant institutional framework of risk management will be constrained.”²⁷⁷ As Hindmarsh explains;

“... for effective participatory transitions or civic trajectories that are not simply add-on components... inclusive participatory approaches need to address the overarching institutional context of the socio-technical system under investigation...”²⁷⁸

- 5.74. There have been attempts to engage with the public around issues of DNA etc., with the HGC Citizen’s inquiry²⁷⁹ and the Trustguide Report.²⁸⁰ Both held focus groups around UK drawn from general public, discussing issues of forensic DNA use and retention, and public trust in technology and data protection. The HGC inquiry led to 29 core recommendations for the HGC to consider in their final report. Recommendations from citizens included a nationwide public awareness campaign and substantive proposals about DNA retention, rules on collecting samples, the governance of the NDNAD and other issues. The HGC argued persuasively that there is a need for in-depth engagement with public at this level, and less reliance on instant ‘opinion polls’ which do not give people time to think about or absorb information required to understand issues.
- 5.75. The Trustguide Report reached similar conclusions on the need to engage at a deeper level with the public. They found that many citizens did not believe the government’s reasons for needing to keep biometric data (though not specifically relating to forensic purposes). Focus group members also tended not to trust the Government’s reported reasons for greater surveillance and data collection and felt that DNA collection by the government (not the police) was the most unacceptable form of data collection. There was apprehension about ‘function creep’ with the retention of biometric data in particular,²⁸¹ apprehension that the European Court of Human Rights considers ‘legitimate’:

“The Court maintains its view that an individual’s concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.”²⁸²

²⁷⁷ *op.cit.* n.274., p307.

²⁷⁸ *op.cit.* n.270., p.280.

²⁷⁹ Human Genetics Commission, ‘A Citizens’ Inquiry into the Forensic Use of DNA and the National DNA Database: Citizens Report’. July 2008.

²⁸⁰ Lacohee, H., S. Crane, and A. Phippen, ‘Trustguide: Final Report’, (Trustguide, October 2006).

²⁸¹ *supra.*

²⁸² *S & Marper v UK*, [2008] para.71.

- 5.76. Bigger political issues (particularly the creation of a national ID card) may be causing a shift in public opinion regarding the capture and retention of personal information. In addition, the use of predictive profiling (mostly in the US), is propagating the idea that certain amount of data could, and will be used against the provider. A series of records that could lead to refusal of rights/ surveillance etc. could make people increasingly nervous about linking of databases and the use of databases.²⁸³ The Royal Academy of Engineers argues that ‘reciprocity’ is essential to establishing and maintaining trust in both public and private sector data collection schemes:

“Data collection and use systems should be designed so that there is reciprocity between data subjects and owners of the system. This includes transparency about the kinds of data collected and the uses intended for it; and data subjects having the right to receive clear explanations and justifications for data requests.”²⁸⁴

However, with regard to forensic bioinformation databases, there cannot realistically be such a degree of reciprocity at the level of the individual. Although some of these requirements should be expected – such as clear information upon bioinformation collection. It may be however that demands could be made for this level of reciprocity at the level of the ‘public’.

- 5.77. The American Public Health Association Code of Ethics stresses that the effectiveness of institutions is reliant upon public trust and reciprocity, and that trust can be dependent upon actions on the part of the institution, including: “...communication; truth telling; transparency; (i.e. not concealing information); accountability; reliability; and reciprocity. One critical form of reciprocity and communication is listening to as well as speaking with the community.”²⁸⁵ The Standing Committee for Youth Justice have warned however, that the issue of ‘public confidence’ in the NDNAD is complex. Some of the reasons for public distrust involve:

“lack of trust in sampling and retention procedures, concerns about how this highly personal data may be used, and the public recognition of the lack of tangible evidence informing how decisions around the NDNAD are made. Evidence of the disproportionate use of the database to record information about certain groups in the population, such as individuals from black and ethnic minority backgrounds, is also of serious concern.”²⁸⁶

²⁸³ There are concerns that linking datasets diminishes privacy as information on individuals becomes centralised and more accessible. A debate in medical research is whether more protections need to be in place to prevent biobanks being accessed by the police – akin to the certificates of confidentiality in the USA.

²⁸⁴ Royal Academy of Engineering, *‘Dilemmas of Privacy and Surveillance’* (RAE, London, March 2007) p.9.

²⁸⁵ American Public Health Association, *‘Code of Ethics’*, available at: www.apha.org/codeofethics/ethics.htm

²⁸⁶ Standing Committee for Youth Justice, *Response to ‘Keeping the Right People on the DNA Database’*, August 2009, para.12.

- 5.78. Underlying such concerns is the wider question of public understanding of the police uses of forensic bioinformation (including the commissioning of research on samples and profiles collected by the police in support of criminal investigations). Thomas and Walport stress that the utility of databases is lessened if the public do not trust the organisations handling the data:

“Only when people better understand what happens to their personal information will they invest more trust in the organisations that process it. And only when levels of trust are suitably high will organisations be able to take full advantage of the potential benefits offered by the use of personal information....”²⁸⁷

Such issues underlie calls for an ‘independent body’ to administer the NDNAD, and several responses to the Government consultation called for the retention of profiles to be subject to the scrutiny of an independent body reporting directly to Parliament, bypassing even the Executive and Ministers.

- 5.79. There remain serious shortcomings in the ways in which ‘forensic’ matters are communicated to the general public. Given the importance of public confidence to the success of policing, more work needs to be done on developing public communication and consultation. This issue has most recently been taken up by the UK Statistics Authority, in their current examination of why crime statistics are not trusted or believed by the public, with a preliminary focus being on the communication of such statistics to the public.²⁸⁸ There are further complications caused by the misrepresentation of forensic science by media outlets. Where there is irresponsible reporting, there is a false impression of what forensic science can achieve and how complex issues like error rates should be understood. As O’Neill states, transparency is only a ‘good’ if the information can be made sense of, and simply demanding more information may not increase trust:

“increasing transparency can produce a flood of unsorted information and misinformation that provides little but confusion unless it can be sorted and assessed. It may add to uncertainty rather than to trust. And unless the individuals and institutions who sort, process and assess information are themselves already trusted, there is little reason to think that transparency and openness are going to increase trust. Transparency can encourage people to be less honest, so increasing deception and reducing reasons for trust: those who know that everything they say or write is to be made public, may massage the truth.”²⁸⁹

²⁸⁷ Thomas, R. & M. Walport ‘*Data Sharing Review*’ (July 2008).p.56.

²⁸⁸ UK Statistics Authority, ‘*Overcoming barriers to trust in crime statistics*’, (December 2009).

²⁸⁹ O’Neill, Onora, ‘The Reith Lectures 2002 – A Question of Trust.’ Lecture Four, available at: www.bbc.co.uk/radio4/reith2002

It is essential that information is from a reliable source that can be checked:

“global transparency and complete openness are not the best ways to build or restore trust. We place and refuse trust not because we have torrents of information (more is not always better), but because we can trace specific bits of information and specific undertakings to particular sources on whose veracity and reliability we can run some checks.”²⁹⁰

- 5.80. If provided with accurate, reliable, and ‘checkable’ information, the public can then be suitably ‘informed’ to consent: “informed consent can provide a basis for trust provided that those who are to consent are not offered a flood of uncheckable information, but rather information on whose accuracy they can check and assess for themselves. This is demanding.”²⁹¹ Both the Royal Academy of Engineers and the Human Genetics Commission have called for greater transparency and provision of information to the public:

“data collection and use systems should be designed so that there is reciprocity between data subjects and owners of the system. This includes transparency about the kinds of data collected and the uses intended for it; and data subjects having the right to receive clear explanations and justifications for data requests.”²⁹²

“A condition of public support and informed debate is that there should be sufficient, reliable information available. Openness (access to information) and transparency with regard to how the information is produced, as well as the amenability of information to non-specialist understanding and appropriate support for the public’s ability to understand and interpret the information, are all important.”²⁹³

- 5.81. There is then a need for a proper communications strategy to dispel myths, and inform and educate ministers; judges; lawyers; and the public, emanating from reliable sources. This should include key processes/ technologies etc. with clear and agreed upon definitions and explanations so as to ensure clarity. For example, all parties will need to agree on what ‘deletion’ or ‘retention’ means in practice, what is ‘familial searching’ etc. (to be understandable by public). Only once the public and stakeholders are all properly informed, and speaking in the same language, will progress be possible toward effective governance that retains public confidence. It may be useful to consider how civil society groups may be informed of strategic developments in forensic science in general and the uses of forensic bioinformation in particular at a relatively early stage – and whether they may have a stronger voice in discussions surrounding these developments. As Irwin states, such ‘openness’: “is not intended to block

²⁹⁰ *ibid.*, Lecture Two.

²⁹¹ *ibid.*

²⁹² Royal Academy of Engineering, ‘*Dilemmas of Privacy and Surveillance*’ (RAE, London, March 2007) p.9.

²⁹³ Human Genetics Commission, ‘*Nothing to Hide, Nothing to Fear?*’ (2009) Para 6.5.

scientific progress, but instead create a more open and reflective culture where new scientific possibilities can be fully realised.”²⁹⁴

- 5.82. Magee stresses that positive attitudes to biometric data for use in public protection are vital: “Ministers need to lead a public debate to help improve public understanding and confidence.”²⁹⁵ There is also need for ongoing engagement with statisticians to work on how forensic science may be clearly explained to juries and legal professionals with minimum risk of confusion. There also needs to be absolute clarity about the potential uses of forensic bioinformation to prevent unauthorised use or ‘mission creep’. This can occur most often where there is confusion or initial lack of clarity over the intended primary functions of the resource. Not that all ‘mission creep’ should be considered negatively:

‘Function creep is often beneficial and has been a means to real progress in many areas of human endeavour. However, where the potential exists for function creep to lead to unwelcome consequences, there is a need for appropriate safeguards. Two safeguards can be applied: the clear and precise definition of the proper function; and effective regulation of use (the second being ineffective without the first).’²⁹⁶

What may be required is further public and parliamentary debate on the legitimate uses of forensic bioinformation, for example, should the NDNAD be used to find or identify ‘missing’ persons?

Integration

- 5.83. As both the Flanagan review and Magee report have stressed, policing takes place within a network of actors and agencies: “Policing is not simply the preserve of the police. Modern policing is carried out in partnership with a wide range of local agencies, from councils to primary care trusts to schools”.²⁹⁷ The use of forensic bioinformation, like any police information, needs to be integrated successfully into such networks, to ensure its effective use. There is also a need to demonstrate that forensic bioinformation is being effectively integrated both within policing domestically; and international systems for crime control; surveillance (intelligence gathering); and movement of persons.
- 5.84. Despite the importance of such integration, there is no clear, or explicit guidance on how forensic bioinformation is successfully, (or should be) integrated into wider policies and practices in policing and criminal justice. How should such information be integrated with other sources/ types of information

²⁹⁴ *op.cit.* n.274, p308.

²⁹⁵ Magee ‘*The Review of Criminality Information*’ (Magee Report, July 2008) Home Office, London, p.88.

²⁹⁶ Human Genetics Commission ‘*Nothing to Hide, Nothing to Fear*’ (London, 2009), para 5.19

²⁹⁷ Flanagan Report ‘*The Review of Policing – Final Report*’ (February 2008) Home Office, p.7.

regularly relied upon by the police, courts, and other law enforcement agencies? The Home Office/ACPO strategy of 2004,²⁹⁸ replacing the DNA Expansion Programme, made a commitment to a more integrated approach to forensic science, particularly in improving the effectiveness of fingerprints. Yet it is difficult to find evidence of any strategy being implemented in practice. The use of fingerprints in particular is becoming increasingly widespread, across several agencies, some that rely upon their own databases, others utilising IDENT1 (i.e. UK Borders Agency *et al*). 'Sharing' of IDENT1 is expected to increase, with the NDNAD the sole preserve of the police, although we have noted in Chapter 4, the emergence of DNA as a border or immigration control measure and UKBA's interest in whether it might assist them to determine asylum applications.

- 5.85. The Bichard Report of 2004 was critical of the ability of police forces to share information on individuals and recommended that the police nationally improve the management and sharing of information and intelligence at both national and local levels. The IMPACT programme responded to this recommendation, creating a statutory Code of Practice on the Management of Police Information (MoPI) in 2005, and the IMPACT Nominal Index (INI), which will allow authorised users in one force to quickly identify which other forces hold information on a person of interest. These will both be supported by the Police National Database (PND) which will provide a national intelligence sharing system. There is a draft Code of Practice on the operation of the PND, which aims to "promote consistent and lawful use of the PND across the Police Service." All forces must comply with the MoPI Code of Practice by 2010, in order to assist with the rollout of the PND, delayed until 2011.²⁹⁹
- 5.86. The Magee Report praised the IMPACT programme stating that "the framework drawn up by the police, the MoPI in 2006, is a good example of efforts to....implement a structure to facilitate the sharing of criminality information."³⁰⁰ While praising these efforts, Magee recalls that there has been significant investment (over £2bn) in IT schemes across the criminal justice sector since 2001, with some benefits for individual agencies, but connections between these systems so that they can 'communicate' have been an 'afterthought'.³⁰¹ The IMPACT programme has also been like many government IT programmes, in that it has had troubles "with delays, funding problems, cost overruns and delivering fewer business benefits than originally envisaged."³⁰² There have also been issues regarding accountability, which has not been a strong feature of major government IT programmes.

²⁹⁸ Home Office (2004) *Confident Communities in a Secure Britain: the Home Office Strategic Plan 2004-08* (London: The Stationery Office) p.73

²⁹⁹ NPIA Website accessed 16 December 2009

³⁰⁰ Magee 'The Review of Criminality Information' (Magee Report, July 2008) Home Office, London p.41

³⁰¹ *ibid.*, p.70

³⁰² *ibid.*, p.69

- 5.87. Recent changes in the organisation of key government departments will impact on policy and practice in forensic science support to policing. Key to these will be the emerging role of NPIA. Existing networks of influence involving the Home Office, ACPO, and as a government owned company, the Forensic Science Service (FSS) and others are likely to be modified by the presence of the NPIA as an agency with a role in both policy making and practice improvement. It will be important for NPIA to effectively integrate the work and interests of a number of scientific, operational and other communities. The bulk of the NPIA budget is spent on the national delivery of services; accordingly the sum available to support the development of strategy and the assessment of potential innovations remains small (and most likely shrinking). Policing and priorities in developing scientific applications need to be subject to ongoing ethical scrutiny, although it is not clear what body exists – or should exist – to assist in such scrutiny. It will be important for the NPIA to effectively integrate the work and interests of a number of scientific, operational and other communities as it seeks to deliver the several work streams of Forensics21.
- 5.88. The number of databases and the organisation of the police and other relevant agencies has leant itself to duplication, with SOCA being a prime example. SOCA inherited over 350 databases from predecessors upon its creation (they are hoping to reduce this to between 50 and 60).³⁰³ The attempt to create an explosion on a Delta Airways flight on Christmas Day 2009 also highlighted the issue of potentially counter-productive duplicity of databases with numerous, vast ‘watch-lists’ in existence around the world with minimal communication.³⁰⁴ The proliferation of data has limited efficient and effective exchange of information between databases, with technological issues often overwhelming. Just domestically, with 43 police forces across the country, this is exacerbated by sheer volume of data, with the police of England and Wales estimated to hold over 70 million operational records across 350 different systems.³⁰⁵
- 5.89. The UK experience has shown that the expansion of DNA retention enabled by legislation in 2001 and 2003 also created the necessity for keeping ‘criminal’ records for those not convicted of a criminal offence. Changes in the DNA and fingerprint retention regime will require the consideration of the necessity for the parallel removal of ‘criminal’ records of those whose DNA profiles and fingerprints are to be destroyed although there is no intention (presently expressed) to return to the ‘weeding’ that was previous ACPO policy. The move to retain all arrest information indefinitely has been supported by the ‘Five Chief Constables’ ruling which found indefinite retention of all PNC records lawful. This emphasises the need for more widespread consideration of the retention of all criminal justice information and what should be the relationship between bioinformation databases and the criminal justice process and public policy.

³⁰³ *ibid.*, p.71

³⁰⁴ ‘World terror watch lists flawed’, *Washington Post* (Online), 9 January 2010.

³⁰⁵ Magee ‘*The Review of Criminality Information*’ (Magee Report, July 2008) Home Office, London p.42.

- 5.90. Magee called for a 'Public Protection Network' (PPN) encompassing an array of agencies, moving from the idea of 'police' data; 'prisons' data; 'immigration' data etc. and promoting the sharing of 'criminality' information under the umbrella of 'public protection' data.³⁰⁶ He calls upon the Ministry of Justice to lead in the area of criminality information, with its portfolio of prisons, probation, courts and criminal justice IT, making it ideally placed for this role.³⁰⁷ With a PPN, Magee believes that there could be strong oversight and governance, permitting the productive exchange of information with connectivity across the various agencies and government departments who deal with 'criminality' information. With strong governance, the public could have confidence in the PPN, and believe "...that action is taken is proportionate to the risks being addressed, that there are sufficient checks and balances in place and that governance arrangements will ensure high standards."³⁰⁸ This could go some way to meeting the request by the Joint Committee on Human Rights, that the government show: "...that any proposal for data sharing is both justifiable and proportionate, and that appropriate safeguards are in place to ensure that personal data is not disclosed arbitrarily but only in circumstances where it is proportionate to do so."³⁰⁹
- 5.91. Magee argued that it is critical that the public have confidence that the PPN is "...collaborating to meet the new challenges posed by advances in criminality information and the problems and opportunities presented by international information."³¹⁰ As the 'Data Sharing Review' by Thomas and Walport (2008) highlighted, there are risks in sharing and also not sharing information: "There are symmetrical risks associated with data sharing – in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data."³¹¹ They also stressed the need for good governance: "It is equally important that such decisions [about sharing personal data] are taken in the context of good mechanisms of governance including transparency, audit and accountability."³¹²

Conclusion

- 5.92. Public trust is an essential precondition for the effective use of forensic bioinformation. The government need trust to enable 'consensus' legislation. The police need trust in order to utilise the technologies and only trust can allay suspicions of 'Big Brother' futures. With trust in the institutions responsible for collecting, using, and governing forensic bioinformation, individuals and

³⁰⁶ *ibid.*, p.90

³⁰⁷ *ibid.*, p.70

³⁰⁸ *ibid.*, p.5.

³⁰⁹ Joint Committee on Human Rights, '*Data Protection and Human Rights Report*' (Fourteenth Report of Session 2007-08) para.14.

³¹⁰ Magee '*The Review of Criminality Information*' (Magee Report, July 2008) Home Office, London, p.5.

³¹¹ Thomas, R. & M. Walport '*Data Sharing Review*' (July 2008).p.i.

³¹² *ibid.*, p.ii.

communities can gain the benefits of these technologies yet still know that respect for human rights and the democratic process remain unchallenged. These are not simply matters of technology and science:

“If we are to design and develop trusted technologies we need to understand the complex inter-relationship between trust, confidence, control and security. The first issue that arises here is the need to understand that this is not simply a technological problem that can be solved in isolation...”³¹³

- 5.93. Securing and maintaining trust in any institutional arrangements requires clear lines of accountability and the possibility of appropriate levels of independent oversight. Sufficient information must be available to enable relevant publics to give support and consent. This information needs to emanate from reliable sources, and be ‘checkable’, and therefore available to external researchers.

“...public confidence is reflected in government policy through legislation and budget. Privacy debates and lingering civil liberty concerns can erode public confidence, and replacement of misinformation with factual DNA information is essential.”³¹⁴

- 5.94. Trust in the operation of forensic databases is especially sensitive to the provision of security and adequate data protection: ‘While it may take years of effective governance to establish institutional trust, it can be wiped out very quickly, however fairly or unfairly, by high profile mistakes or accidents.’³¹⁵ There cannot be room for failure as this will be followed by a catastrophic loss of confidence in those who manage such data as well as in the management procedures themselves. Clarity of purpose and aims secured through proven quality standards and the oversight of such standards will also contribute to the healthy regard necessary for these technological innovations to be used for the achievement of the public good.

³¹³ Lacohee, H., S. Crane, and A. Phippen, *Trustguide: Final Report*, (Trustguide, October 2006).p84.

³¹⁴ INTERPOL. *Handbook on DNA Data Exchange and Practice* 2nd edn. (2009) available at www.interpol.int p.49.

³¹⁵ Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance* (RAE, London, March 2007) p.44.

Summary and A Proposal

Beyond *S & Marper*

- 6.1. England & Wales is clearly at a crossroads, with significant decisions to be made regarding the direction now to be taken about the collection, retention and use of forensic bioinformation. Recent debate remains dominated by the exchange of bold claims made for the usefulness of forensic bioinformation (e.g. “The NDNAD continues to provide the police with the most effective tool for the prevention and detection of crime since the development of fingerprint analysis over 100 years ago.”³¹⁶) rather than by the careful analysis of robust data. A further limitation on the ability to conduct the much demanded ‘informed debate’ is that the potential for, and limitations of, the use of bioinformation globally in law enforcement and related activities have been inadequately discerned.

- 6.2. After years of developments in forensic bioinformation occurring away from public gaze, with minimal parliamentary debate or media attention, the ruling at the European Court of Human Rights in *S & Marper* has thrown a spotlight on forensic bioinformation databasing. While the NDNAD was increasingly featuring in studies of ‘surveillance’,³¹⁷ and also had been the subject of reports by the Nuffield Council on Bioethics, the Human Genetics Commission, and numerous papers by Genewatch, Liberty, Justice *et al*, it has now received renewed and highly focused government attention. Since the ruling in December 2008 there have been two government Bills containing proposals on forensic bioinformation preceded by two consultation papers. The Home Affairs Select Committee also conducted a brief inquiry into the National DNA Database (although they did not mention IDENT1 in their inquiry).

- 6.3. This period of consultation and deliberation, has ceased for now, with the legislative response of the UK Government apparently dealt with in the ‘wash-up’ period of Parliament before the general election, with the passing of the Crime and Security Act 2010. However, it is clear that the ECtHR judgment will have ongoing ramifications, with its requirement to radically reshape the forensic bioinformation regime of England & Wales, and will also serve to shape emerging regimes elsewhere in Europe. However, the debate has focussed upon the ‘retention’ of forensic bioinformation, since the court in Strasbourg ruled that UK police powers to retain bioinformation breached human rights.³¹⁸ There is perhaps then a lost opportunity if the debate cannot move beyond this one narrow issue of retention (and the retention of the bioinformation of ‘innocent’ individuals at that).

³¹⁶ Foreword, CC Neyroud, NDNAD Annual Report 2007-09, p.4.

³¹⁷ i.e. Home Affairs Committee 5th Report of Session 2007-08 ‘*A Surveillance Society?*’ HC 58-1 (The Stationery Office, London, June 2008) ; House of Lords Select Committee on the Constitution: ‘*Surveillance: Citizens and the State*’ HL Paper 18-1 (The Stationery Office, London, February 2009).

³¹⁸ In particular, the right to privacy found in Article 8.

- 6.4. The European Court of Human Rights, in reaching their unanimous decision, were scathing of the UK's 'indiscriminate and blanket regime' of retention, stating that the government needed (and had failed) to provide 'weighty reasons' for their policies and practices. They also stated that the UK bore a 'special responsibility' as a country at the vanguard of forensic bioinformation use. Most other EU countries have not followed England, Wales and N. Ireland in implementing such an extensive retention regime. The initial response of the UK Government to the judgment was met with derision (not assisted by the scandalously poor quality 'evidence base') and their initial proposals for changes were dropped from the Policing and Crime Act 2009. Amended proposals were brought forward in primary legislation - the Crime and Security Bill - in the dying days of parliament before breaking for a general election.
- 6.5. The issue dominating debate and government efforts since the *Marper* judgment is the 'blanket and indiscriminate' retention regime for DNA and fingerprints. In both the ruling and subsequent debate, comparison with the Scottish retention regime has been a constant feature. This might reflect views about a procedural difference (retention in the absence of conviction only, in effect, after case by case scrutiny by a procurator fiscal in Scotland,)³¹⁹ as well as the variation between outcomes following arrest that trigger retention in England and Wales compared with Scotland. The government are clear in their intention to avoid individual case by case decisions, except possibly in 'terrorist' cases where a Chief Constable can authorise ongoing retention 'in national security interests' for two years, which is then renewable.
- 6.6. The Government have attempted what they have designated a 'scientific' approach to retention in order to demonstrate the 'utility' of retaining bioinformation in crime detection, rather than an ethical, or legalistic, or human rights approach (for instance, relying on ethical, legal, or human rights based tenets or arguments). The difficulty is that the evidence produced for this 'scientific' approach has failed expert scrutiny and so has not been able to provide a base upon which to build proposals.
- 6.7. The Council of Europe Committee of Ministers (which monitors the responses to ECtHR judgments and sees that they have effect), raised a series of questions regarding the governments' proposals in the Policing and Crime Bill.³²⁰ In their assessment of the provisions set out in the Bill, they asked whether the proposed retention regime was proportionate and struck a fair balance between public and private interests. They specifically pointed to the proposal to retain DNA from arrestees for non-serious offences, stating that this did not conform to the requirement of proportionality. They also stated that the

³¹⁹ See Section 18A (1) of the Criminal Procedure (Scotland) Act 1995 (as amended): 'that criminal proceedingswere instituted.....'.

³²⁰ The response to *S & Marper vs UK* was considered at the 1065th Meeting, September 2009.

provisions for children and adults were too similar and did not respond to the requirements of the judgment in *S & Marper*. Similarly, the continuation of the mechanism for the destruction of profiles did not respond to the Court's wish for an independent review mechanism and was an ineffective response. The Committee also criticised the 'evidence' used to inform the proposals, stating:

"Given the UK's claimed 'pioneer role', reliance only on academic studies, two of which do not relate to the United Kingdom and an approach to those studies which appears to rest on the principle that unconvicted individuals will commit criminal offences, do not appear sufficient to justify retention periods which do not appear to be in conformity with the Court's judgment."

- 6.8. In *W v The Netherlands*,³²¹ the ECtHR held that retention of DNA for convicted persons was acceptable where it was retained "for a prescribed period of time dependent on the length of the statutory maximum sentence that can be imposed for the type of offence committed." This was in direct contrast to the approach of the UK government, which "does not consider retention on the basis of any link with the maximum sentence but rather on the possibility of future offending." Indefinite retention of DNA from convicted offenders does not itself have unqualified support, with many questioning retention in cases which are very minor, or in which DNA plays no part. The Equalities and Human Rights Commission have called into question the legality and usefulness of retention in some cases, i.e. a conviction for a minor offence (perhaps single offence) of insurance fraud.
- 6.9. In a subsequent meeting in December 2009, the Committee of Ministers referred to the revised proposals in the Crime and Security Bill, but still noted that "a number of important questions remain as to how the revised proposals take into account certain factors held by the European Court to be of relevance for assessing the proportionality of the interference with private life here at issue, most importantly the gravity of the offence with which the individual was originally suspected, and the interests in deriving from the presumption of innocence." They also queried where further proposals were in relation to "the institution of an independent review of the justification for retention in individual cases."³²²
- 6.10. It should be possible to develop a retention regime that is Article 8 compliant. Some technological protections may afford a more 'privacy friendly' regime and such (albeit partial) solutions should be considered. It must also be borne in mind that any changes resulting from the *Marper* judgment will impact on the private organisations that hold samples on behalf of Chief Constables (the

³²¹ *W vs The Netherlands* (application No. 20689/08, decision of 20/01/2009)

³²² 1072nd (DH) Meeting, December 2009. Decisions Adopted at the Meeting. Section 4.2.

forensic service providers) and methods will have to be put in place to ensure compliance with agreed understandings. The regulations regarding the uses made by private organisations of such samples, along with their holding of identifying information need to be reconsidered (along with the bioinformation data held by other agencies such as the Crown Prosecution Service (CPS)). It is also important that any revised retention regime keeps in mind the significance of DNA and fingerprint records for the successful investigation of crime, especially those crimes – like violent offences and serious sexual assaults - in which biological evidence can be central to an investigation and prosecution. Consideration should be given to collecting and retaining the best possible data on uses of the NDNAD after any legislative changes. Only in this way will it be possible to measure the effect of the changes and monitor satisfaction with the resulting regimes in case there is demand for further changes, or indeed future challenges to the legality of forensic bioinformation use.

- 6.11. The issue of requests for removal has been the focus of the Home Affairs inquiry, prompted by Damian Green MP's arguments that a 'postcode' lottery exists depending upon which force 'owns' the DNA and their rates of acceding to requests. The NDNAD Ethics Group has repeatedly drawn attention to their dissatisfaction with the 'removal' process, preferring: "an independent, statutory appeals procedure in order to provide an effective remedy".³²³ Without such a process, they argue that there is a risk that the process is; "inconsistent and discriminatory...In particular there is no element of independence that is at the heart of a requirement to provide an effective remedy under the ECHR".³²⁴ Liberty go further in questioning: "why a person must make out 'exceptional circumstances' before deletion can be considered. This test bears no relationship to the tests of necessity and proportionality found in the Human Rights Act or to the Data Protection Principles...."³²⁵
- 6.12. There is still then no satisfactory consensus on how best to approach questions on the use and retention of forensic bioinformation. The preference in England and Wales has been to begin by focussing on police powers and on questions of 'utility', a preference which has generated piecemeal legislation largely uninformed by more general considerations. An alternative is to begin by considering principled questions of human rights. The European judges have reminded us of the necessity of justifying the police retention of bioinformation which in many circumstances can be seen as a breach of privacy, but acknowledged there were differences between the three categories of personal data that would require careful scrutiny although their ruling did not consider in detail the differences between DNA profiles, samples and fingerprints.

³²³ NDNAD Ethics Group *Response to "Keeping the Right People on the DNA Database"* August 2009, p.7.

³²⁴ *ibid.* p.8.

³²⁵ Liberty, *Response to "Keeping the Right People on the DNA Database"* August 2009, p.29.

- 6.13. In determining whose information (including bioinformation) should be retained when the activity giving rise to an arrest has not been subject to judicial deliberation, it may be necessary to improve the quality of information about the circumstances of any arrest and charge as well as the reasons for failing to proceed with a case, or failing to obtain a successful prosecution of a suspect offender. The use of arrest as the 'trigger' for taking bioinformation could be the critical issue (rather than subsequent retention). Indeed, in their response to the government's consultation, the NDNAD Ethics Group states that:

"The use of arrest as the trigger for retention of those unconvicted encompasses many people who are not subsequently either charged or proceeded against.... We seriously question whether this is a sufficient basis for justifying retention. We therefore recommend that further research needs to take account of these points in order to reach a better understanding of the proportionality of appropriate 'triggers'³²⁶

- 6.14. Soothill and Francis explain why the arrest 'trigger' may be inappropriate, but more importantly, why 'arrest hazard rates' are not satisfactory indicators of offending behaviour, and therefore a base on which to make predictions of future offending (and therefore justify retention):

"While police arrests are not whimsical, they come at the beginning and not the end of the criminal justice process. Some people are disproportionately at risk of being taken into questioning by the police and being arrested. In contrast, a conviction is the outcome of the evidence being tested in court. In fact, arrests are useful indicators of police action, but not of guilt. Re-arrests are dangerous indicators and making arrests the pivotal criterion encourages the notion that we are moving towards becoming a police state."³²⁷

- 6.15. It may be true that, particularly when dealing with young offenders, a swift and appropriate sanction may be preferable to waiting for a court disposal, indeed significant efforts have been made to increase non-court disposals to avoid lengthy delays and this may have beneficial impacts on both the court system and the offender, suggesting that dependence upon a court to decide upon 'guilt' may not always be ideal. Better knowledge of offending patterns as well as potential 'dangerousness' needs to be subject to consideration if something more discerning than 'blanket retention' is to be acceptable. In the absence of such data, 'blanket retention' may continue to be seen as providing the best opportunities for the identification of offenders through fingerprints and DNA profiles, and may support calls for a 'universal' database.

³²⁶ *op.cit.*, n.326. p.8.

³²⁷ Soothill, K. & Francis, B. 'Keeping the DNA Link' (17 July 2009), *New Law Journal*, 1021-1022: 1021.

- 6.16. New considerations arise when the collection and retention of forensic bioinformation is viewed from the perspective of crime prevention rather than criminal prosecution. The traditional repertoire of checks and balances function largely in relation to prosecuting accused persons within the context of criminal trials. However, the modality of crime prevention is informed by a different set of considerations about checks and balances, and this is not always realised. Without such consideration there is a real danger of function creep, and it is easy to lose transparency in the proprietary – and legality - of such uses.
- 6.17. In recent debates there has been a tendency to attribute the sustained drop in crime since 1997 in part, to the use of forensic DNA. This in part has intimated that the DNA database has some ‘deterrent’ effect which has led to a decrease in offending. However, there is no evidence of the deterrent value of the NDNAD. While it is feasible, if difficult, to assess the utility of DNA in investigations and prosecutions, measuring any ‘deterrent’ effect would be extraordinarily difficult, if not impossible. Arguments therefore that the retention of DNA can ‘deter’ must necessarily always fail without any possibility of evidence to support such claims.
- 6.18. Indeed, sociological theories of the power of ‘labelling’³²⁸ may be relevant to debates around bioinformation retention, which would lead to diametrically opposed conclusions regarding the ‘deterrent’ effect of retention. Labelling theory would suggest that by attaching to an individual labels such as ‘future suspect’ or ‘potential criminal’, as is arguably achieved by the Government’s current policy of assessing the ‘risk’ posed by arrestees as warranting retention for six years, you actually increase the likelihood that the individual will ‘live up’ (or in this case ‘down’) to the label. According individuals (particularly young people) status as a future offender creates the perfect conditions for these individuals to fulfil these prophecies (the ‘self-fulfilling prophecy’ a well established phenomenon in psychology).
- 6.19. It could be argued, with the support of such theories, that by treating people as ‘future’ criminals (or ‘pre-suspects’³²⁹), you might make it more likely that this will become true. Newspaper reports have already highlighted an instance where the presence of a DNA entry on the PNC, brought to a police officers’ attention through mobile checking of a driver’s identity while on patrol, led to differential treatment and increased suspicion.³³⁰ It cannot be discounted that

³²⁸ There is an extensive literature on this approach to criminology that addresses the issues, *inter alia*, of the subjectivity of the processes that are sometimes used to identify deviant behaviour, and the consequences of this for both society and the labelled individual. Key texts include, Becker H.S. (1963) *Outsiders*, Cohen, S.(1972) *Folk Devils and Moral Panics* and Plummer K (1979), ‘Misunderstanding Labelling Perspectives’ in Downes, D. And Rock, P. (eds.) *Deviant Interpretations*.

³²⁹ Lynch, M., Cole, S., McNally, R. And Jordan, K. (2008) *Truth Machine: The Contentious History of DNA Fingerprinting* (Chicago and London, The University of Chicago Press), p. 152.

³³⁰ ‘DNA Database – Head to Head’, BBC Website, available at: http://news.bbc.co.uk/2/hi/uk_news/8354740.stm accessed 25 April 2010.

the behaviour of others alters when interacting with an individual who has their details retained on the PNC, retention that will be necessary due to the requirements of the bioinformation retention regime. It is already clear that such retention of details on the PNC has an adverse impact on visa applications, and potential employment.

- 6.20. It is necessary to distinguish between efforts to regulate the retention of DNA profiles and fingerprints taken from known individuals and those collected during the search of crime scenes. It generally seems to be the case that there is no restriction on the retention of the latter kind of information regardless of the apprehension or prosecution of criminal suspects, albeit that in England and Wales, these data are removed from databases (a situation that should also be addressed but currently does not feature in debates).
- 6.21. There are also significant linguistic issues at stake when questions of forensic bioinformation (and other kinds of police-relevant information) retention are raised. There are problems in translating key terms across jurisdictions, and there are also issues surrounding the uses of polyvalent terms like 'innocent' when political arguments take place. Decisions about the proper balance between liberty and public protection need to take into account the differing meanings attributed to words like 'innocent' and 'serious crime' for example, by a range of police and other actors. This linguistic and definitional aspect is particularly relevant as the definition of a 'serious crime' can be subjective. Whilst some may relate this term to offences of murder, rape, robbery etc, a 'minor' domestic violence case may be reported after years of abuse and may be the precursor to more serious domestic violence if not treated as a 'serious offence' from the outset.
- 6.22. The comment by ECtHR about the 'blanket and indiscriminate' nature of the retention regime need not necessarily result in the rule base approach advocated in *Keeping the Right People on The DNA Database*, which proposed that DNA profiles should be retained automatically in a narrower range of circumstances and for a shorter time period than at present. This has been presented as similar to Scots law with simply a wider range of circumstances that might give rise to retention (and a longer retention period). Crucially this misses the really distinguishing feature of the Scottish arrangements: the case by case scrutiny by a Procurator Fiscal and the scope for judicial supervision. This analysis is reinforced by the information about a more selective sampling policy followed by the police themselves. During the initial seminar participants were reminded that the Nuffield Council on Bioethics had been advised during the preparation of its report that the scrutiny of individual decisions was unaffordable. Further discussion elicited comments that because in Scotland a smaller number of profiles are processed, it is easier to make case by case decisions about retention. The comparatively lower levels of recorded crime,

higher clear-up rates and the more generous number of police officers in Scotland (per 100,000 of population) supports this observation.

- 6.23. During the Commons Committee stage of the Crime and Security Bill, ACPO stated that retention proposals based on the Scottish arrangements should be rejected for England and Wales for reasons of additional cost. Instead, ACPO argued for simple retention rules based on offence categories with deletion via computer algorithm, enabling the whole process to be managed by algorithm. The Scottish system, with its emphasis on an examination of individual circumstances, 'was rejected because it would take up an inordinate amount of police resources'.³³¹
- 6.24. It was also suggested during the third seminar that Scotland might be able to establish a central clearing house for such decisions, but that to put such a system in place in England and Wales would be more difficult. This was not followed up at the time (indeed it was a final remark at the end of a long day). It is possible, however, that this was not raised as a financial or logistical issue, but one relating to the notional ownership of samples or profiles. Certainly the legislation hurriedly pressed upon Parliament prior to dissolution appears to offer a hybrid of uncertain central influence over decision making by individual chief constables in respect of the DNA profiles.
- 6.25. These arguments fail to address the point that the real lesson from Scotland may be that it offers a model of individuals within the criminal justice system exercising professional judgment on a case by case basis. Such an approach would meet concerns about both excessive retention and the problem of formulating rules to predict potential future harm. For example, if a person was arrested but it soon appeared that it was a case of mistaken identity or to ensure that bioinformation was collected from a potential witness for elimination purposes, it should be a simple matter for those handling the case to have the profile deleted or retained temporarily as a volunteer sample. The individual concerned should not have to initiate a deletion process and might reasonably expect that no trace of the sample having been taken remains on the PNC. In contrast, even when no charges were laid or proceedings were discontinued, information about an individual may be retained for good reasons. The latter circumstances were recognised as an important lesson from the failure to take action that might well have prevented the double murder at Soham and is reflected in the individual case management of information set out in the MOPI code. Neither a hybrid of central and local decision making, nor deletion by algorithm are acceptable substitutes for the individualised decision making at all stages of the criminal justice system and local procuratorial or judicial review available to some six million fellow UK citizens.

³³¹ Public Bill Committee, 26 January 2010, Q93 and 97-100.

6.26. If decisions are taken at the right time it is difficult to see how an approach should lead to higher costs. Ironically, the exercise of greater discretion by individual police officers was the main element in evidence given to the Public Bill Committee by the Government's 'Police Bureaucracy Czar' and the Chairman of the Police Federation when testifying about another aspect of the legislation now enacted as the Crime and Security Act 2010. In contrast, ACPO's stance appears to demonstrate insufficient concern for both legitimate concerns about privacy and the deskilling of the police work. On the latter issue, the Chairman of the Police Federation commented:

'Although we are very good at following the quantitative, measuring approaches, what matters to the public is not the quantity of what we do, but the quality. It is no accident that we have inspectors and superintendents in the police service. They actually used to inspect and superintend what those under their control did. We have lost that to some degree. The quality of what officers are doing seems to be less important to those in command than the quantity, and we have to get away from that.'³³²

6.27. Finally, there is some evidence to support the contention made in this report that a margin of appreciation based on no more than a survey of legislation is a possibly more fragile basis for reaching views on proportionality than is suggested in *Marper*. Scotland may have achieved a balanced approach to retention issues that still need to be settled south of the border. This appears to have been as much a chance outcome, as one of good professional and political judgment. It is far from clear, however, from reading recent debates at Westminster that what we would argue is the defining characteristic of Scots law in this area, the exercise of individual discretion, has been fully understood.

Evidence and Assessment

6.28. Whilst forensic science in general is a major police consumable,³³³ it is also highly vulnerable to arbitrary cuts during budgetary crises.³³⁴ The changing regime for funding expenditure on forensic science has already forced the police to question whether existing or expanded forensic spending represents good value, and there is not always support amongst senior levels within the police service for the maintenance of the priority accorded to forensic science in

³³² Public Bill Committee, 26 January 2010, Q 15.

³³³ Accounting for approximately half the ICT spend and slightly less than on transport: Home Office Police Science and Technology Strategy 2008-2009 (London: Home Office, 2004) p26.

³³⁴ Often due to a lack of scientific awareness among senior police officers, see: Blakey, D. (2000). *Under the Microscope*, (London: Home Office), Blakey, D. (2002) *Under the Microscope Refocused* (London: Home Office) and Coleman, D. (2004) 'Beyond DNA in the UK – The Police Perspective', in Townsley, M. and Laycock, G. (eds) Forensic Science Conference proceedings: *Beyond DNA in the UK – Integration and Harmonisation* (London: Home Office), pp 9-10.

recent years compared with other policing budget items.³³⁵ Other agencies, such as the Crown Prosecution Service, also face significant decisions regarding their future requirements for the provision of forensic bioinformation, decisions that need to be informed by a sound understanding of the implications of 'staged reporting' arrangements for the production and utilisation of forensic science results. Such decisions necessarily impact upon the whole legal system with regard to the direction of limited financial resources.

- 6.29. Expenditure on DNA and fingerprints like all other activities within the criminal justice system should, wherever possible, be assessed for its effectiveness in line with other budget items and subject to cost-benefit analysis, even though such assessments are notoriously difficult to carry out.³³⁶ Failing this the police and the NPIA should at least demonstrate that the collection and use of forensic bioinformation is being organised optimally, that they do not divert resources from budgetary items that are proven to be more beneficial, and that police internal forensic organisation and procurement of external forensic services are cost-effective. It is necessary then accurately to assess the opportunity costs of expenditure on forensic bioinformation, its impact upon the state's ability to offer justice to all citizens, and its implications for the wider resourcing of the criminal justice system.
- 6.30. In summary, arguments over fundamental issues concerning the collection, retention and use of forensic bioinformation as well as disagreements about how key problems are to be resolved, continue to be poorly supported by a credible evidence base on which to ground important decisions. Instead, after an unconvincing consultation exercise, the current UK government appears to have abandoned the idea, discussed when we began our work, of publishing a forensic science White Paper. It has recently conceded that there is a need for new primary legislation dealing with forensic bioinformation collection, retention and database governance, which resulted in provisions in the Crime and Security Act 2010.

Internationalisation & Exchange

- 6.31. With increasing mechanisms, and imperatives to exchange law enforcement data, internationally and particularly within the EU, and the extent to which decisions about this have to comply with rules and policies negotiated with other governments or have been influenced by bodies outside this country, an

³³⁵ Peter Neyroud, NPIA Director, 31st March 2008, in evidence to Home Affairs Select Committee inquiry into the '*Surveillance Society*'. Available at:

http://www.parliament.uk/parliamentary_committees/home_affairs_committee.cfm .

³³⁶ The most recent work assessing value for money and the ability of economic analysis to inform decision making within policing was highly cautious about the application of such techniques (see Stokedale, Whitehead, & Gresham (1999) Police Research Series Paper 103 '*Applying Economic Evaluation to Policing Activity*' (London: Home Office), since then there has been a major increase in data to which such techniques might be applied.

examination of the UK situation can no longer be undertaken without consideration of the international context in which policing and efforts to maintain 'security' are now played out. The Secretary General of Interpol argued that DNA profiling is 'a discovery that has benefited mostly the wealthiest of countries' and yet there was a clear need for greater international cooperation using this forensic technique.³³⁷ Despite this exhortation, little has been published about the scale of international cooperation or the effectiveness of recent and emerging measures taken to share police information, forensic or otherwise, across national boundaries.³³⁸ There are also pressing, but as yet unresolved scientific, and policy issues, brought into stark relief by the Prüm Treaty, which automates the exchange of some forensic bioinformation.

- 6.32. International cooperation involving the exchange of forensic bioinformation is in its infancy. While information is scarce, the amount of cooperation appears to be occasional even when investigating serious crimes. Within the European Union this might change as a result of the Prüm Treaty, although the introduction of technologically advanced searching systems and databases alone will not necessarily result in major increases in activity. The Council of the European Union has already sought to restrict the extent of future searching under Prüm, presumably to prevent analysts being overwhelmed by search requests and the need to verify results. This state of affairs may not be in the interests of justice. There is a consistent, but almost anecdotal view held by experienced investigators about the value of routinely exchanging bioinformation for dealing with transnational crime. In the absence of statistical analysis and independent case evaluation however, it is difficult to reach an informed view about the optimal scale and arrangements for such cooperation.
- 6.33. Currently there are many jurisdictional differences in practice both within common law jurisdictions and between common and civil law jurisdictions. In some jurisdictions (e.g. US and Canada) legislation operates at both State and Federal level. Whilst complexities arise from this, there are many jurisdictions in which such levels exist and it seems unlikely that relevant local agencies in such jurisdictions will easily surrender sovereignty to national bodies. However, the interoperability of NDNAD and the Scottish database, together with the ability of the forensic services of the two administrations and Scottish criminal justice colleagues to manage different retention regimes on a large scale (as indicated in Table 4.1) is clear evidence that forensic cross-jurisdictional cooperation can be successfully managed on a large scale despite legal differences. While this report identifies some gaps and lack of consistency in the data and suggests where research is urgently needed, the scale and detail of the interoperability analysis indicates that the NDNAD has set an example of greater openness nationally and internationally for criminal justice databases,

³³⁷ Noble, R.K. (2007) Opening Remarks at 5th International DNA users' conference for investigative officers, 14 November 2007 (Lyon, Interpol) published at www.interpol.int .

³³⁸ Smith, D. (2007) Uncorrected Transcript of Oral Evidence to House of Commons Home Affairs Committee, 23 January 2007, published at www.publications.parliament.uk .

including the exchange of information about fingerprints, and possibly genetic collections in the genetic medical research and health fields.

- 6.34. Any consideration of the multinational exchange of forensic bioinformation is unlikely to give rise to novel technical issues. In some countries the size of AFIS databases and the use of different multiplex systems or differences within the same jurisdiction present the same problems as those that have to be resolved before international cooperation can be successful. It helps to identify with greater clarity some of key strategic issues facing the forensic community. This is of little value, however, in the absence of institutions with the resources and authority to foster greater national coordination.
- 6.35. The key issue is higher risk of erroneous or missed identifications arising from essentially the same type of problems in respect of both fingerprints and DNA: the recovery from the crime scene of incomplete (both), degraded (DNA), damaged (fingerprints) or distorted (fingerprints) material. Experts working in both disciplines face similar questions about contamination or poor recovery, transmission or storage techniques, but the main risk of missing a correct match or declaring an incorrect identification stems from specific reasons inherent to each discipline. The cognitive issues arising in respect of the identification of similarities and differences in patterns by fingerprint examiners are undoubtedly intensified by the scale and speed of modern database algorithmic searches, and the ability of individual examiners to understand and manipulate the operations of different proprietary systems.
- 6.36. For UK DNA international casework the chief obstacle now and increasingly in the future are the different multiplex systems used across the globe, the known technological obsolescence of SGM+ and the considerable scientific difficulties in moving to a sufficient number of overlapping loci with the other widely used systems developed in the USA and China. These problems will undoubtedly increase, as the Government has admitted, because of its decision to no longer retain DNA samples. The initial trials involving Germany and the Netherlands under Prüm have demonstrated that with many countries obtaining valid results from cooperation depends on the ability to reanalyse cellular material taken from a known individual.

Governance and Accountability

- 6.37. Irrespective of views on the *Marper* judgment, there is a clear consensus that the advances made technologically in the forensic use of DNA in England and Wales have not been balanced by equal attention to the governance of this emerging field of activity. This can be contrasted unfavourably with the arrangements in Canada and some European countries. While it remains

questionable whether direct and periodic legislative scrutiny, along the lines of the Canadian model, is the best and most informed approach for ensuring public trust in the nature of future trajectories in the forensic use of bioinformation, it remains perhaps preferable to foregoing any scrutiny at all. Self-regulation is problematic and self-regulatory systems are prone to failure, pointing to the need for stronger safeguards to be in place.

- 6.38. There remain questions over how to regulate the taking of bioinformation by the police (not considered in *Marper* or in ensuing debates). It is not mandated and often occurs in cases where apparently a complete irrelevance, while it is not taken in other instances, such caprice adding to public mistrust. Sensitivities surrounding retention are exacerbated by the difficulties encountered by the public in finding out their rights when having/ had DNA taken, in particular, getting data removed, a point forcefully made by the recent Home Affairs Committee Report on the NDNAD.
- 6.39. A proper response to *Marper* must also include an effort to define key terms ('transparency', 'accountability', 'safeguards', 'proportionality' etc) in a way that establishes clear general principles for the governance of forensic bioinformation in the UK. Innovations in current practice can then be interrogated and positioned properly by reference to those principles. There is also a need to think more generally about 'data about individuals' rather than simply 'bioinformation'. This means consideration of what kinds of forms such data can take, where such data should be stored, how they should be accessed, by whom and for what purposes. There needs to be recognition of different levels of sensitivity and significance and not develop regimes which constrain less intrusive forms and uses simply because some other forms and uses may be especially contentious.
- 6.40. Whatever governance arrangements are put in place, it is crucial that public confidence and trust remain the touchstones for 'success'. The UK Statistics Authority, in their interim report on crime statistics, suspect that there is a wide mistrust of official information, and argue that the way that information is reported is critical to public perceptions and confidence:

"Trust is compromised if official statistics are not produced in a way that is professionally independent, and seen to be independent... But trust can also be undermined by confusion and by the misuse of the statistics, whether the misuse occurs inside or outside the Home Office. It is also possible that the recent controversies about the use of research evidence (in respect of drug classifications and the DNA Database) may have an impact on trust in statistics."³³⁹

³³⁹ UK Statistics Authority, '*Overcoming barriers to trust in crime statistics*', (December 2009), p.11

6.41. Trust in the use of forensic bioinformation has been hindered by the lack of, or flawed research, which is then misrepresented or used to mislead. This has sometimes exaggerated the impact of the NDNAD and does little to explain the value of forensic bioinformation (including the value of fingerprints). The use of emotive anecdotal cases and statements invoking 'public protection' with almost meaningless numerical data, serves only to confuse, and removes from consideration the impact on individuals and on human rights, which is the 'balance' that *Marper* demanded. There has as yet been scant attempt to develop a human rights based approach to forensic bioinformation in the UK, with strong governance at its core. If public confidence is to be maintained in the future of forensic bioinformation, the issues outlined in this report, including the production of robust research data, the creation of effective governance regimes, undertaken within a framework that takes seriously the international context, could be considered essential starting points.

A Proposal

6.42. The formulation of legislation for the governance and operational use of bioinformation has not been central to this study. Nevertheless, we closely observed the passage of the Crime and Security Act 2010 and this has informed our work. There are significant doubts about the durability of this legislation. A considerable weight of expert opinion suggests that the retention regime therein would not withstand judicial scrutiny. In view of this, we conclude this report with a brief consideration of the objectives that might underpin revised legislation in the new Parliament and provide an illustration (*not* a recommendation) of what a reformed system might look like.

6.43. Various problems inhibited the emergence of a coherent, comprehensive and effective response to *Marper*. The political and institutional considerations are dealt with in our summary account of the passage of the Act (paragraphs 1.12 – 1.20) and our concerns about the possible misinterpretation of the lessons from Scotland are set out at paragraphs 6.22 – 25. This final section approaches the issue differently by suggesting that the starting point to further legislation should be a clearer and more convincing demonstration of the objectives and technical arrangements that might ensure the success of new legislation. Underlying this is our belief that further discussions about the response to *Marper* need to dispel the various myths woven in this context about measures to protect rights being inimical to a criminal justice system capable of detecting and dealing with offending behaviour.

6.44. New legislation, if developed with integrity and open-mindedness could achieve a greater degree of public confidence (from both the rights and utility perspectives). It should contain clear principles with precise arrangements to be put in place and tested incrementally. This process might be initiated by the

creation of an independent statutory governance body, whose first task would be to implement satisfactory arrangements for the management, and when required, the destruction of tissue samples taken from known individuals and the DNA profiles analysed as a result of such actions. We suggest that there are four principles that should underpin the preparation of new legislation:

- Every effort should be made to ensure that the new legislation is likely to withstand judicial challenge on 'blanket and indiscriminate' grounds and that, for this purpose, proper consideration should be given, *inter alia*, to whether this requires an approach based on a case by case scrutiny of retention decisions in the absence of a conviction or where a conviction has been quashed on appeal.
- The legislation and its implementation, including risk assessment and optional appraisal studies, should be sufficiently robust and comprehensive to minimise the risk of later changes both in response to the UK suffering serial judicial reversals on the retention issue or recognition within the UK that the present system is inefficient in both operation, incapable of ensuring a uniform quality in the use and management of all forms of forensic bioinformation and police information generally, and lacks sufficient transparency to ensure public confidence in terms of both rights and utility.
- The new arrangements should provide the discretion necessary for investigators to retain and share forensic bioinformation and police information when there is a professional need, and that the exercise of such discretion will be subject, in line with the MOPI code, to regular and effective professional review and audit and, for issues affecting the retention of bioinformation, any challenges before an independent tribunal.
- The general operation of the new arrangements and individual decisions should be informed and regulated by the independent statutory oversight of all forms of forensic bioinformation and, possibly in due course, police information generally. This should be based on effective audit arrangements, adequate data collection and publication, the commissioning of research and ultimate accountability directly to Parliament.

6.45. We have formed many views on the future of forensic bioinformation during this project but we single out the following as some of the immediately relevant:

- The potential shortcomings of the Crime and Security Act 2010 are illustrated by the apparent lack of consideration given to the fact that convictions may be overturned on appeal. For this reason alone, it appears improbable that the recently enacted arrangements will not be

repealed or amended in the new Parliament irrespective of any further judgment in Strasbourg.

- The great advantage of the Scottish case by case approach is that it could never be described as 'blanket and indiscriminate'. Retention in all cases reflects a considered individual judgment with independent oversight.
- The Government estimated that the cost of changing the information held on NDNAD and NAFIS to implement the reforms in the Crime and Security Act 2010, excluding sample destruction, in excess of £50m.³⁴⁰ Little attention has been given to the possibility that if the new Act is judicially reversed, further costly changes may be needed. This may help to put the refusal - based on assertions about affordability – to consider a case by case approach, in a more accurate economic perspective.
- There are likely to be major advantages in being able to detect crime if retention decisions were to be included within a case based and MOPI regulated process. This would integrate the management of retained bioinformation with other police information about individuals who had not been convicted of an offence. By comprehensively combining information it would assist officers when making decisions to retain or destroy bioinformation, both initially and periodically in the reviews required under the MOPI code. Such decisions would be unconstrained by rigid rules about the suspicions of any specific types of offence that may have resulted in arrest. Instead individual officers would be allowed to make a professional decision about an individual's behaviour following an arrest through to conviction, acquittal or the overturning of a conviction on appeal. Such a system would recognise the professional skills of police officers and emphasise the trust that society has in their personal integrity rather than the inferior management of important but highly variable information by machine.
- If the police are already MOPI compliant, other than for the cost of introducing such changes, there should not be a major increase in cost. In preparing an illustration of how the system might operate we fail to see how this cannot be incorporated within the decision making and recording processes happening now at key stages in an investigation: arrest, the laying of charges, the initiation and continuation or discontinuation of proceedings, the verdict and appeal decisions. In the longer term a system that integrated all forensic bioinformation and PNC management with MOPI would presumably be more cost effective, as well as more efficient, than the present dispersed arrangements for the governance of DNA profiles, fingerprints and other MOPI information. This would be consistent with recommendations in key studies from Bichard Report

³⁴⁰ Home Office (2009), *Impact Assessment of the implementation of the S & Marper ECtHR judgment regarding DNA profiles, DNA samples and fingerprints retention* published at www.crimereduction.homeoffice.gov.uk/crimeandsecuritybill/ .

(2004) to the Flanagan *Review of Policing* (2008), which have been concerned with avoiding 'gaps in intelligence sharing' and duplication.³⁴¹

- Even under the Act of 2010 can the system really operate chiefly by the application of an algorithm? Conviction would require a management decision to convert a temporary period of retention to a permanent one. Similarly acquittals, if they are to be taken into account, would require a further intervention. If the system has to be designed to respond to such instructions, other decisions could be notified to NDNAD management, as part of the routine paperwork at two other key decision points: if it is decided not to charge the arrestee or to discontinue proceedings.
- The burden of paperwork could be reduced by default deletion and destruction procedures. For example, if the police have not informed the NDNAD and IDENT1 database management that proceedings have been instituted within a set period after the notification that charges have been laid, the information would be automatically deleted. This would also provide a safeguard against the failure discovered by HMIC to comply with earlier deletion legislation because the discontinuation of proceedings and acquittals had not been notified by the police to the database operator.³⁴² A further safeguard against a reoccurrence of this problem would be provided in this respect by holding any information relating to unconvicted or acquitted individuals on a separate MOPI database.

6.46. While the authors cannot claim any expertise in systems design, Figure 6.1 sets out an option for how such arrangements might be introduced. The existing NDNAD Ethics Committee might form the nucleus of the proposed audit and ethics board and members of the NDNAD Strategy Board would become part of the new executive body. It will be noted that we consider that the audit and ethics body should be responsible for initiating research, as well as approving external research requests and that its statutory audit functions should extend to record keeping, database operations and the storage of samples by all accredited forensic suppliers. This body should produce an annual report for Parliament with sufficient data to describe the routine operations of the new system, the basis volumes of business and results achieved, and the volume of and results obtained from international cooperation.

³⁴¹ Muir, R. (2009) *Arrested Development: Unlocking change in the police service* (London, IPPR), pp. 33-34.

³⁴² In the 1990s there were major problems in removing profiles that should have been deleted under the current law from the then quite small NDNAD. As a result, a large number of samples and profiles – estimated at 50,000 but acknowledged to be perhaps higher – were being held on the NDNAD unlawfully. See Williams, R., and Johnson, P. (2008) *Genetic Policing* (Cullompton: Willan), p. 84.

Figure 6.1: An option for arrangements for case by case decisions about retention, indicating mandatory and discretion decision points within the criminal justice system. Mandatory information requiring action by NDNAD operational staff is in solid green lines and optional police decisions requiring action by NDNAD in dotted green lines. In the absence of action by the police to order retention, in the absence of a conviction report, the profile will be deleted from the database within a specified time of the original arrest or the latest discretionary retention decision.

