Title: The UK National DNA Database: implementation of the Protection of Freedoms Act 2012

Authors: Aaron Opoku Amankwaa, Carole McCartney

PII: S0379-0738(17)30557-1
DOI: https://doi.org/10.1016/j.forsciint.2017.12.041
Reference: FSI 9123

To appear in: *FSI*

Received date: 5-6-2017
Revised date: 22-11-2017
Accepted date: 28-12-2017

Please cite this article as: Aaron Opoku Amankwaa, Carole McCartney, The UK National DNA Database: implementation of the Protection of Freedoms Act 2012, Forensic Science International https://doi.org/10.1016/j.forsciint.2017.12.041

The UK National DNA Database: implementation of the Protection of Freedoms Act 2012

Aaron Opoku Amankwaa [a *] (Email: aaron.amankwaa@northumbria.ac.uk)

Carole McCartney [a]
(Email: carole.mccartney@northumbria.ac.uk)

[a] Science and Justice Research Interest Group, School of Law, Northumbria University, Newcastle Upon Tyne, UK, NE1 8ST

*Corresponding Author:

Aaron Opoku Amankwaa

Phone: +447442929880

Email: aaron.amankwaa@northumbria.ac.uk

Highlights

- Protection of Freedoms Act 2012 regime improves National DNA Database performance
- Protection of Freedoms Act 2012 strengthens genetic privacy protection of individuals

Implementation challenges of PoFA leads to unlawful forensic DNA data retention/non-retention

Abstract

In 2008, the European Court of Human Rights, in *S and Marper v the United Kingdom*, ruled that a retention regime that permits the indefinite retention of DNA records of both convicted and non-convicted ("innocent") individuals is disproportionate. The court noted that there was inadequate evidence to justify the retention of DNA records of the innocent. Since the *Marper* ruling, the laws governing the taking, use, and retention of forensic DNA in England and Wales have changed with the enactment of the Protection of Freedoms Act 2012 (PoFA). This Act, put briefly, permits the indefinite retention of DNA profiles of most convicted individuals and temporal retention for some first-time convicted minors and innocent individuals on the National DNA Database (NDNAD). The PoFA regime was implemented in October 2013. This paper examines ten post-implementation reports of the NDNAD Strategy Board (3), the NDNAD Ethics Group (3) and the Office of the Biometrics Commissioner (OBC) (4). Overall, the reports highlight a considerable improvement in the performance of the database, with a current match rate of 63.3%. Further, the new regime has strengthened the genetic

privacy protection of UK citizens. The OBC reports detail implementation challenges ranging from technical, legal and procedural issues to sufficient understanding of the requirements of PoFA by police forces. Risks highlighted in these reports include the deletion of some "retainable" profiles, which could potentially lead to future crimes going undetected. A further risk is the illegal retention of some profiles from innocent individuals, which may lead to privacy issues and legal challenges. In conclusion, the PoFA regime appears to be working well, however, critical research is still needed to evaluate its overall efficacy compared to other retention regimes.

List of Abbreviations

ASBCPA: Anti-Social Behaviour, Crime and Policing Act 2014
BFEG: Biometrics and Forensics Ethics Group
BRU: Biometrics Retention Units
CED: Centralised Elimination Database
CJA: Criminal Justice Act 2003
CJPA: Criminal Justice and Police Act 2001
CJPOA: Criminal Justice and Public Order Act 1994
CPIA: Criminal Procedure and Investigation Act 1996
CSA: Crime and Security Act 2010
CTDNAD: Counter-terrorism DNA Database
ECtHR: European Court of Human Rights
FSPs: Forensic Science Providers
MPS: Metropolitan Police Service
NDNAD: National DNA Database
NDU: National DNA Database Delivery Unit
NEG: NDNAD Ethics Group
NFA: No Further Action
NGS: Next Generation Sequencing
NIDNAD: Northern Ireland DNA Database
NSD: National Security Determination
OBC: Office of the Biometrics Commissioner
PACE: Police and Criminal Evidence Act 1984
PED: Police Elimination Databases
PNC: Police National Computer
PND: Penalty Notice for Disorder
PoFA: Protection of Freedoms Act 2012
SDNAD: Scottish DNA Database
UKAS: United Kingdom Accreditation Service

Keywords: National DNA Database, retention regime, genetic privacy, public security, match rate, Marper ruling

1 Introduction

The United Kingdom National DNA Database (NDNAD) was established in April 1995. It is the oldest national forensic DNA database in the world and the largest measured by the proportion of citizens on the database (over 8.2%). It holds DNA data from all police forces in England and Wales as well as data from: the Northern Ireland DNA Database (NIDNAD); the Scottish DNA Database (SDNAD); and DNA profiles from the Crown Dependencies (Isle of Man, the Bailiwick of Jersey and the Bailiwick of Guernsey). As at September 2017, the NDNAD held 6,112,274 subject reference profiles (of which 5,317,752 are known individuals due to duplication) and 575,923 crime scene DNA profiles.[1] The primary purpose of the database is to identify unknown offenders as well as serial offenders by linking

different crimes. Another potential value of the database is the possibility of analysing crime patterns,[2] providing intelligence that can assist law enforcement agencies in prioritising resources. Although less than 1% of recorded crime is detected using the NDNAD, the detection rate of crimes that involve DNA matches on the database is higher than crimes without DNA evidence.[2,3]

The criminal justice value of retained DNA profiles can be illustrated by cases such as those of Keith Samuels[4–6] and that of Joseph Kappen.[7] Keith Samuels was a resident of Northampton who raped 7 different women from 1984 to 1990. He was apprehended in a cheque fraud case in 1998 when his DNA was then sampled by the police. On loading his profile to the NDNAD, a match was found between his reference sample and the crime scene profiles from the rapes stored on the database. This led to his subsequent conviction and nine life sentences in 1999.

In the triple rape and murder case of Joseph Kappen, forensic investigators utilised a then innovative sub-programme of the database called familial searching. This involves searching the database for closely matched profiles to identify potential relatives.[8] The crimes took place in 1973 and the cold case was re-investigated in 2000. Forensic scientists used the Low Template DNA technique[9] to generate DNA profiles from crime scene samples. A search of the database returned zero hits after which a familial search was launched. The stored DNA profile of Paul Kappen, a car thief, was found to share half of the offender's profile. Further investigation led to his deceased father Joseph Kappen whose identity as the offender was confirmed following DNA analysis of samples recovered from the teeth and femur of his exhumed body.

The retention regimes for DNA data from England and Wales, Northern Ireland and Scotland are independent of each other though they share similarities and currently, the law in England, Wales, and Northern Ireland is the same. Different legislative regimes governing DNA data retention have been implemented for the England and Wales NDNAD since 1995. A summary of the different legislative regimes enacted or proposed for the retention of forensic DNA profiles is presented in Table 1. The first governing statute, the Criminal Justice and Public Order Act 1994 (CJPOA),[10] amended the Police and Criminal Evidence Act 1984 (PACE) to enable the databasing of DNA profiles. The CJPOA permitted DNA records (both DNA samples and derived forensic DNA profiles) of all individuals convicted of a recordable offence to be retained indefinitely. The Act generally required DNA records of those who had never been convicted of a criminal offence, to be considered "innocent", and thus deleted after the conclusion of an investigation or any proceedings. All data retained on the database were subject to speculative searching against other profiles.

The implementation of the CJPOA regime encountered procedural challenges such as repeated sampling of offenders and suspects, and potential risks to public security due to legal technicalities.[3] In the murder case of *R v Weir*,[11] for example, a conviction was overturned by the Court of Appeal due to the unlawful retention of the subject's DNA profile, which had initially led to the identification of the offender. This resulted in public security concerns and led to the amendment of the law by the Criminal Justice and Police Act 2001 (CJPA) and subsequently, the Criminal Justice Act 2003 (CJA).

This second retention regime permitted the indefinite retention of DNA records of convicted individuals, those acquitted of an offence or whose proceedings against them had been discontinued, and those charged or arrested for a recordable offence. The implementation of the second regime was perceived as a simple system to administer,[12] potentially minimising repeated sampling and allowing the police to gather and retain data of the "active criminal population". Additionally, an expanded database was perceived to have a deterrent effect, albeit there did not exist evidence to support this potential benefit.[2] Critics of this second regime noted the inversion of the presumption of innocence and the risk of creating a "suspect society".[13,14] Moreover, there was no justification provided for the retention of data from innocent individuals,[15] that is whether it contributed to the performance of the database and aided the detection of crime.

In 2008, the European Court of Human Rights (ECtHR) in *S and Marper v the United Kingdom*[16] ruled that this represented a "blanket" and "indiscriminate" retention regime which did not strike a fair

balance between an individual's right to privacy and the public interest. This case involved "S" (a juvenile) and Mr Marper, who were separately charged in 2001 with attempted robbery and sexual assault respectively. S was acquitted and Mr Marper's case was discontinued, but their DNA and fingerprint records were retained. A request for the deletion/destruction of their biometric records was declined and subsequent appeals to the English Courts were unsuccessful. At the EtCHR, the judges unanimously decided that the expansive regime infringed upon Article 8 rights to privacy, noting the inadequate justification for the retention of "innocent" samples and profiles (the "*Marper gap"*). This ruling led to the development of new retention rules set out in the Crime and Security Act 2010 (CSA)[17] (see Table 1) which were informed by consultations and research carried out by the Jill Dando Institute of Crime Science. This research attempted to determine the risk of re-arrest among unconvicted individuals (~52% in 6 years),[18] yet it was heavily criticised, primarily because the data relied upon was unclear.[15] Due to a change in government, the CSA regime was never brought into force. Instead, the Protection of Freedoms Act 2012 (PoFA) was developed by the subsequent coalition government to govern DNA and fingerprint data retention in England and Wales.[19]

The PoFA rules in summary include: the destruction of DNA samples after profiling or within 6 months of collection; indefinite retention of convicted individuals' DNA profiles; and deletion of profiles from innocent individuals after the conclusion of an investigation or any proceedings.[20] The exceptions to these general rules include: temporal profile retention periods for some first time convicted minors; those charged or arrested for a qualifying (serious) offence; those issued with a penalty notice for disorder; or on national security grounds. Since the implementation of PoFA in October 2013, over 1.7 million forensic DNA profiles from "innocent" individuals have been deleted and over 7.7 million DNA samples have been destroyed post-DNA profiling.[21] Critical reviews of the PoFA regime highlight the potential incommensurate treatment of public and private interests and the continuing lack of "weighty reasons" for the retention of data from innocent individuals.[15,22,23]

Two independent statutory bodies have specific oversight functions for the UK National DNA Database: the NDNAD Strategy Board ("Strategy Board") (now the National DNA and Fingerprint Databases Strategy Board) and the Commissioner for the Retention and Use of Biometric Material (Biometrics Commissioner).[24,25] The statutory role of the Strategy Board is provided in section 24 of PoFA, being required by law to provide guidance on the retention and destruction of DNA profiles, governance rules for the database, and produce an annual report about the exercise of its functions.[20] The statutory functions of the Biometrics Commissioner are set out under section 20 and 21 of PoFA. The Commissioner's role is to keep under review the retention and use of DNA and fingerprints under the PoFA retention regime. Further, the Commissioner is also required by law to provide an annual report. Another independent advisory non-departmental public body with an oversight role is the NDNAD Ethics Group (NEG) (now changed to the Biometrics and Forensics Ethics Group (BFEG)).[26,27] The NEG operates on a non-statutory basis and its vision is to ensure that the operation of the NDNAD is ethical. The NEG also produces an annual report about its work and recommendations. This paper thus reviews these annual reports of the NDNAD Strategy Board, the NDNAD Ethics Group and the Office of the Biometrics Commissioner (OBC) published since the implementation of PoFA. The purpose of the review is to identify the potential benefits, challenges or gaps, risks, and emerging issues associated with the new DNA data retention regime under PoFA, which has not yet been subjected to critical review.[12,25,28]

2 Methodology

A total of ten annual reports of the three independent bodies with specific oversight functions for the UK National DNA Database were analysed for recurrent themes on the benefits and best practice, challenges, risks, and emerging issues associated with the implementation of PoFA. The ten reports were published after implementation of PoFA (October 2013). The review includes three annual reports of the Strategy Board (2013/14, 2014/15 and 2015/16), three annual reports of the NEG (2014, 2015 and 2016) and three annual reports (2014, 2015 and 2016) and a supplementary report of the Biometrics Commissioner (Table 2). The general principles of thematic synthesis of literature and qualitative data was used to generate the key themes in the review.[29–32] The iterative process involved the coding of text, sorting of relevant codes into key themes, comparing the generated themes to the original report and then between the reports for similarities and differences.

3 Results

The key themes identified from the ten reports are summarised in Table 3 below. The thematic synthesis of the reports identified a total of twenty-one key themes in relation to forensic DNA. Comparatively, the reports of the Biometrics Commissioner produced more themes (n=20) than the other independent bodies (Strategy Board (n=5), NEG (n=7)). This is explained by the comprehensive and detailed nature of the Commissioner's reports, as well as the dedicated focus upon PoFA (as this Act gave rise to the statutory duties of the OBC) and the retention, use, international sharing and destruction of DNA profiles and fingerprints, and overall compliance with the PoFA. The Strategy Board and NEG reports also cover other issues unrelated to PoFA and thus did not contribute so many of the key themes.

3.1 Benefits of PoFA implementation

The implementation of the PoFA regime has resulted in several benefits noted in the reviewed reports. The new regime is reported to have strengthened the level of protection of the privacy interests of innocent individuals.[12,24–26,28,33–36] For example, in cases where the retention of DNA profiles of unconvicted individuals is deemed necessary, the PoFA procedures require corroboration of the suspicious involvement of the individual.[35] Further, the process has reinforced the requirement to provide suspected individuals with detailed information on the grounds for the retention of their data and their right to make representations.[35] Most of the reports indicate a wide acceptance of the PoFA regime as a more proportionate system.[12,24–26,28,33–36] The implementation of the new regime has increased awareness of ethical and legal considerations, including privacy rights, proportionality and necessity. The new system has established a critical monitoring and assessment of legal compliance with PoFA when retaining DNA profiles, in order to fulfil obligations upon the State to respect human rights (Human Rights Act 1998), as demanded by *Marper*. Interestingly, some of the reports

recommend the need to apply the PoFA rules to other new biometric technologies.[12,26,28] The 2015 annual report of the Ethics Group specifically recommends that "the retention times directed in the Protection of Freedoms Act 2012 for the retention of DNA samples and fingerprints should also be applied to the retention of custody images."[26] Whilst the retention of custody images is considered by some as less intrusive than DNA, the Ethics Group believe their retention raises significant privacy concerns. Hence, the need to apply the PoFA rules to custody images.[26]

Match rate is an output metric used to assess the performance of the NDNAD. It measures the chance that a crime scene profile loaded on the NDNAD matches a subject profile.[24] Since its establishment in 1995, the NDNAD has provided the highest match rates (61.9% in 2013-14,[33] 63.2% in 2014-15,[34] and 63.3% in 2015-16[24]) with the introduction of the PoFA regime. The current match rate is also reported to be one of the highest across DNA databases in Europe. The 2014 NEG report notes that "the initial impression is that the removal of large numbers of "unconvicted" profiles has not significantly affected the effectiveness of the database, although it is too early to draw firm conclusions."[35] Most of the reports emphasise that the new system seems to have had a positive impact on the match output of the database.[12,24,25,28,33–35]

Another potential benefit of the PoFA system, as suggested in the 2014 OBC report, is that it has significantly decreased costs, and resources required for storing millions of samples indefinitely under previous regimes.[12] The new system has also led to the introduction of PoFA compliance checks by the United Kingdom Accreditation Service (UKAS) and the Biometrics Commissioner for accredited Forensic Science Providers (FSPs) and police forces, respectively.[12,28] This has mandated the introduction of adequate processes by FSPs and police forces to demonstrate compliance with the new regime. Although compliance checks have not been completed for all police forces, the Office of the Biometrics Commissioner asserts that the bulk of samples/data that need to be retained or destroyed have indeed been retained or destroyed.[12,25,28]

Finally, another practical value of the new system is the opportunity for case reviews.[12,28] Best practice has been identified when Biometrics Retention Units (BRU) are established within police forces.[28] A BRU can assess cases and identify those that may benefit from extended biometric data retention. This has led to the identification of shortcomings in some cases. For example, the BRU of the Metropolitan Police Service (MPS) identified a sexual assault case with a suspect for whom a No Further Action (NFA) entry had been made, where they should have been charged (they were subsequently convicted).[12] Other cases where no biometric data were taken have also been identified and the data of the individuals involved have now been obtained and added to the NDNAD.

3.2 Challenges of the PoFA implementation

3.2.1 Police National Computer (PNC) limitations

The automatic deletion of biometric records on the NDNAD is driven by the Police National Computer, which contains records of all arrestees. One of critical challenge with the implementation of PoFA thus arises from limitations with the configuration of the PNC programme.[12,25,28] The 2014 and 2015 reports[12,28] of the Biometrics Commissioner extensively detail the technical and procedural challenges encountered with the PNC.

Firstly, the PNC programme requires manual entries to be made to drive the "automatic" deletion of data on the NDNAD.[12,28] Although the programme could be improved to support the new system, its high-cost and resource implications have compelled the police to settle for the current "compromise".[12,28] This has led to some erroneous retention of biometric data.[12,28] The guidance provided requires forces to confirm the legality of every match generated before progressing an investigation.[12,28] Secondly, the PNC is not compatible with the PoFA concept "the conclusion of the investigation of an offence" which triggers the automatic deletion of data from innocent individuals.[12,28] Another compromise has been found by substituting with the similar concept of the "NFA" entry made on the PNC.[12,28] For protracted investigations where an individual is "NFA-ed" but extended retention is deemed necessary, the current guidance requires the Biometrics Commissioner to

provide discretionary retention advice.[28] Thirdly, the efficiency of the PNC is determined by the timeliness and accuracy of entries made by forces. Delays in updating the PNC or erroneous entries due to misunderstanding of retention markers have resulted in unlawful retention or loss of data in some instances.[12,25,28]

3.2.2 Non-engagement of police forces with PoFA

Another critical challenge with the implementation of the PoFA system is poor engagement by police forces. The reports of the Biometrics Commissioner emphasise the limited applications made by police forces (23 out of 43 forces in 2015/16) in the case of individuals arrested for a serious offence (section 63G of PACE).[12,25,28] Although the expected annual applications were estimated at ~1000 per year, there was a total of 386 applications from October 2013 to December 2016 (91 in 2013/14, 118 in 2014/15 and 177 in 2015/16), with over 75% (290) of applications by the MPS alone.[25,28] Further, there were only 6 applications made for those charged with qualifying offences (Section 63F (7) of PACE) – all made by the MPS.[25,28] The reasons for non-engagement include: financial and resource demands; dissatisfaction among some forces about the transfer of risk from legislators; the perception that individuals can be sampled in future offences when they become suspects; and difficulties in identifying cases or understanding the circumstances in which retention is required.[25,28]

3.2.3 Limited data on case resolution rate

Most reports noted the limited data to adequately demonstrate the effectiveness of the new retention regime.[12,24,25,28,33–35] The 2014 NEG report[35] proposed methods to address this deficit, including the collection of data on the size of each retention category, the match rate of the database before and after PoFA implementation, and the match rate for each retention criteria. The report indicates that there has been some progress made in this respect although a post-legislative scrutiny of the PoFA system is yet to be carried out, and the Biometrics Commissioner's reports have emphasised that such a review should be informed by rigorous research into the efficacy of the new retention regime.[12,28]

The reports of the Strategy Board include data on the output of the database (i.e. the annual match rate) and "positive match outcomes" including charges/summons, caution/warnings, issuance of a penalty notice for disorder (PND) and community resolution (41.6% in 2014/15; 50.4% in 2015/16).[24,34] Further statistics are reported in the third report of the Biometrics Commissioner which shows that DNA is linked to case outcome in only 0.3% of all recorded crime (0.9% for theft of vehicles, 1.4% for domestic burglaries, 0.6% for rapes and 8.4% for homicides).[25] There is still no information, however, on how DNA contributes to case resolution.[25] In this regard, the Ethics Group have recommended the collection of data on NDNAD match conviction rates in sexual assault cases.[26,36] One difficulty in determining these rates is that the DNA match is normally just one element in a larger body of evidence or, because of the different circumstances of each case, it cannot be easily determined if the DNA evidence alone "led" to a conviction.[25,35] Moreover, offenders may have been identified by other means and the DNA match may have only confirmed identity.[25] The 2015 NEG report indicates preliminary research has been initiated to address this issue.[26]

3.2.4 Database contamination and error rates

The Ethics Group notes that some "contaminated data" may be retained on the NDNAD, a situation which undermines principles of data protection and the goal of ensuring proportionality.[35] This problem is partly due to the non-routine checking of the Police Elimination Databases (PED). An ongoing project to establish a Centralised Elimination Database (CED) that will be subject to weekly searching is proposed to address this issue.[24,26,34,36] Another problem is the limited information on the scale of errors related to the use of DNA.[25,35] Information on the scale of errors is important because the rate of subject sampling error has currently been found to be "unacceptably high".[25] Issues related to DNA sampling errors and database contamination are currently under investigation.[24–26]

3.2.5 Inadequate enforcement of PoFA rules for CTDNAD

The Counter-terrorism DNA Database is a standalone database that stores DNA profiles related to counter-terrorism policing. Prior to the third report of the Biometrics Commissioner, the holdings of

the CTDNAD was unknown.[25] Available data now indicates the CTDNAD holds 608 DNA profiles of which 11% (65) are from unconvicted individuals.[25] There has been a "governance deficit" in the operation of the CTDNAD; resulting from inadequate enforcement of the PoFA regime.[12,26,28,35,37] Hence, a significant data due for deletion may still be retained.[37] The difficulties with the operation of the CTDNAD are compounded by expiry problems due to procedural delays in sample transfer from ports (entry points to the country) to the Secure Operations – Forensic Services (formerly known as Counter Terrorism Forensic Services – the unit that operates the CTDNAD).[37] Other issues include delays in referral of cases to the Joint Forensic Intelligence Team (the team that makes National Security Determination (NSD) Assessments) and provision of summary assessments and incorrect estimation of expiry dates due to incompatible IT-systems.[37] Steps are being taken to minimise the risks associated with these issues and since July 2016 no data has been lost.[25,37] Finally, the Biometrics Commissioner notes the "(…) difficulty of obtaining reliable statistical information about the biometric material on the CT databases [including the CTDNAD] that is subject to the requirements of PoFA".[37] This means that some material that requires an NSD application may have been overlooked or data that requires deletion may have been retained.[37]

3.2.6 Limited statutory guidance on discretionary retention

Statutory guidance on retention decisions under section 63G of PACE is considered to be limited.[12,28] Further, there is no indication of the extent of disclosure when informing unconvicted individuals on the grounds for data retention.[12,25,28] A consultation to develop core principles and guidelines was carried out in May 2013.[38] Detailed processes consistent with the guidance of the NDNAD Strategy Board have now been developed.[12,25,28] This considers factors such as the seriousness of the offence, characteristics of the individual, value, proportionality and necessity of retention, and whether the individual has been informed of the retention of data and their right to make representations.[12,25,28]

Another issue with discretionary retention is that there is no legal definition or guidelines for the section 63E of PACE concept "the conclusion of the investigation of the offence".[12,25,28] This makes it difficult to determine when an application for extended retention is necessary.[12,28] The substituted procedure of the NFA entry made on the PNC for arrestees is not without problems.[28] The discretionary retention procedure is perceived to be complicated and a "bright-line rule" may be preferable because it is easier and cheaper to implement.[28] A bright-line rule is when, for example, samples or data of those charged with a qualifying offence are automatically subjected to three years' retention. It is also suggested that the abolition of discretionary retention under section 63G and 63F(7) of PACE may not significantly endanger public security or decrease the efficiency of the NDNAD.[28]

Other guidance gaps with discretionary retention are resampling of individuals after data deletion and the PoFA requirement for a causal relationship between sampling arrest and any conviction.[12,33,34] For the former, initial guidance policy permitted resampling by consent when an investigation is reopened. Currently, section 144 of the Anti-Social Behaviour, Crime and Policing Act 2014 (ASBCPA) permits resampling without consent. For the causal relationship requirement, new section 145 of ASBCPA now provides that there is no need for a sampling arrest to lead to charge or conviction before retention, allowing a sample taken in one offence to be used for another offence.

3.2.7 Misapplication of CPIA exception

The Criminal Procedure and Investigation Act 1996 (CPIA) exception permits extended retention of DNA samples for prosecution disclosure purposes.[12,25,28] Changes under PoFA considered the CPIA exception for DNA profiles for all offences and DNA samples of individuals involved in a serious offence. A wider application of the CPIA exception for samples was introduced by section 146 of the ASBCPA. This applies to only the relevant offence for which the sample was taken. It is noted that oversight of the CPIA exception is inadequate, and the rule may be misapplied by some forces due to uncertainty of the circumstances requiring its application.[12,25,28] A new system introduced in January 2016 requires all "CPIA samples" to be subjected to quarterly review by police forces.[25]

3.2.8 Inadequate rules for volunteer sampling and samples

Another challenge with the implementation of PoFA is the lack of adequate rules for volunteer or elimination samples.[12,26,28,35] This oversight has resulted in prolonged retention of volunteer DNA samples since they are subjected to indefinite retention – a situation that may discourage individuals from donating samples for use in criminal investigations.[28] The third report of the Biometrics Commissioner indicates this issue has been resolved and volunteer samples are now subjected to PoFA rules (since January 2016).[25] A second issue with volunteer sampling is the lack of information provided to volunteers on consent forms regarding the grounds for retention of their DNA.[28] The Ethics Group "still remains concerned that the consent forms used do not show that the rights of individuals concerned are sufficiently protected".[35] This concern was raised in the first NEG report published on July 21, 2008, prior to the implementation of PoFA. An appropriate consent form was finalised by relevant stakeholders in 2015 and this was introduced in January 2016.[25,26,28,36]

3.3 Risks and emerging issues

3.3.1 Public security risk due to non-retention of data

The complexities of discretionary retention have led to, and will continue to lead to, the potential deletion of some DNA profiles that need to be retained.[12,25,28] This problem may negatively impact upon the efficient detection or prevention of crime in the UK. Another matter of concern is legal, technical and resource issues related to data retention of individuals convicted of serious offences outside the UK. The biometric records (including DNA) of thousands of individuals who have convictions from another country have not been subjected to indefinite retention (as permitted by law) and hence data have been deleted or will be deleted from the database, exposing the public to potential security risks.[12] Another difficulty is that, though permitted under the law, sampling arrests on the grounds of having a conviction from outside England and Wales may constitute a greater breach of privacy than retention of material already obtained. This legal issue has recently been resolved through the Policing and Crime Act 2017.[25]

Finally, although the current PoFA system seeks to ensure proportionality between public and private interests, the Biometrics Commissioner notes that:

> "Absent indefinite retention of every arrestee's biometrics, there will inevitably be times when crimes will go undetected or un-prevented because material obtained from individuals who have been arrested but not convicted is not retained for an indefinite period."[28]

3.3.2 Breach of privacy due to unlawful retention

Whilst the bulk of data that are required to be deleted from the NDNAD have been deleted, challenges with the PNC, misapplication of the CPIA, oversight, and limited enforcement of rules for the CTDNAD have led to the potential unlawful retention of data from thousands of individuals.[12,25,28,37] These retained data are also subjected to automatic speculative searching the same as lawfully retained samples. Existing guidance to mitigate this privacy risk is the requirement that forces check the lawfulness of any NDNAD matches before acting upon them.[28] However, police forces have adopted a policy of using unlawful matches for intelligence purposes, an emerging issue which the Biometrics Commissioner indicates may potentially breach section 63T of PACE.[28]

3.3.3 Contention surrounding future benefits of retention

An emerging contention arising from the implementation of the PoFA regime is whether the retention of data from innocent individuals under section 63G(2) of PACE will contribute to the prevention or detection of crime in future.[12,25,28] Whilst some forces believe that retention for cases involving domestic violence for example, will be useful in detecting or preventing similar future crimes, the Biometrics Commissioner notes that "there will rarely be compelling reasons to believe that the retention of the material at issue may assist in the prevention or detection of crime".[12] The reasons given are that such suspects will readily be identified by the victim or will be obvious suspects and the police will be able to sample them at that time.[12]

3.3.4 Need for expansion of qualifying offences

Section 65A of PACE provides the list of qualifying offences that merit extended biometric data retention for innocent people. The Police and Criminal Evidence Act 1984 (Amendment: Qualifying Offences) Order 2013 expanded this list but excluded the possession of prohibited weapons and the importation of Class A drugs and their possession with intent to supply.[12,28] It is indicated that Parliament was to consider a legislative instrument covering those offences and other offences of a similar substance in mid-2016.[28] The Commissioner's third report indicates this legal issue is still live.[25]

3.3.5 Retention after a match but without arrest

Following an NDNAD match, current police policy permits retention of DNA profiles without an arrest. There is no time limit for how long the sample can be retained whilst the match is being investigated. The Biometrics Commissioner has indicated that this policy breaches sections 63D(3), 63E, 63P and 63T(2) of PACE which seems to proscribe the investigation of an offence without an arrest.[12,28] An amendment to the law and/or police policy has been suggested to resolve this issue but this is yet to be considered and implemented.[12,25,28]

3.3.6 Complex NSD process

A National Security Determination (NSD) is made by a Chief Constable in writing to extend retention of data of unconvicted individuals on national security grounds.[12] This NSD expires after two years and can be subjected to two years' renewals afterwards. Individuals whose data are considered for an "NSD retention" are not informed about the existence of an NSD or the reasons for retention.[12] The statutory guidance on NSDs is provided by the Secretary of State, in consultation with the Biometrics Commissioner and the Lord Advocate. The role of the Biometrics Commissioner is to review the NSDs and the use of retained material.[12,25,28] The NSD process runs on a dedicated IT system but the Biometrics Commissioner has no automatic access to the NSD applications' underlying information, a situation described as time-consuming and labour intensive.[12,25,28]

The 2014 report of the Biometrics Commissioner indicates that the current statutory guidance on NSDs could be more useful if illustrative examples that demonstrate when an NSD is appropriate are included.[12] Further, changes introduced by section 146 of the ASBCP should be included in the guidance.[12,28] Other specific issues that make the NSD process complicated include sample/data transfer delays; use of IT system that is incompatible with PoFA – a problem which has led to the calculation of wrong expiry dates for some data; NSDs made by officers of insufficient rank in a few cases; and reliability issues with statistical information on the number of individuals whose data are being held on national security issues.[12,28,37]

3.3.7 Resource needs for compliance checks

Following the implementation of PoFA, arrangements were made for UKAS to include PoFA compliance checks in its existing annual assessment scheme for Forensic Science Providers (FSPs).[12,25,28] This arrangement is yet to be formalized.[25] Whilst an assessment by UKAS was considered for police forces, this was perceived to be unnecessary and disproportionate among stakeholders.[28] Hence, the Biometrics Commissioner has decided to carry out this duty. About six PoFA compliance checks for police forces had been carried out as at the 2014/15 fiscal year.[28] The third report of the Commissioner indicates a transition to an internal PoFA compliance checks by police forces.[25] This internal system will be evaluated by the Commissioner to assure PoFA compliance by forces. It is emphasised that additional resources will be needed to carry out PoFA compliance checks effectively.[25,28]

3.3.8 Limited statutory guidance for new genetic technologies

The NEG reports emphasise the need for proper guidance and regulations for the introduction of Y-STR profiling and databasing, and DNA phenotyping or massively parallel sequencing (also known as next generation sequencing (NGS)).[26,35,36] A comprehensive ethical impact assessment has been proposed on this issue.[26,35] Further, a wide consultation and debate has been recommended to evaluate

the ethical issues associated with these genetic technologies.[26,35,36] Some of the ethical issues include the possibility of searching for genetic links among males using Y-STR profiling and discriminatory genetic investigation against males.[35,36] The NGS technology can facilitate the prediction of the physical characteristics of individuals including eye and hair colour, age, ancestry and geographical area of origin, and health or disease risk.[26]

4 Discussion

The aim of this review was to identify the benefits, challenges, risks, and emerging issues associated with the implementation of the PoFA DNA retention regime. The key themes and findings identified from the analysed reports are discussed together under each topic below.

4.1 Benefits of PoFA implementation

Against the backdrop that forensic DNA retention has been subjected to political influence and restrictions by country specific laws, there is need to establish standards to safeguard the privacy of individuals and the safety of the public. This is particularly important with the increasing need for data exchange among different organisations, the increase in cross-border police investigations and the demand for international collaboration in law enforcement.[39–41] The new retention regime introduced by PoFA takes consideration of the principles of proportionality and necessity as emphasised in the *Marper* decision.[16] Though some practical benefits have been realised, there are still gaps that need urgent attention.

In 2014, Wallace *et al*[42] carried out a global review of DNA database legislation, focussing on human right standards for the effective operation of forensic DNA databases. The review concluded that there is a growing global consensus to exclude non-convicted individual's DNA records from databases. A previous survey by the Metropolitan Police Authority Civil Liberties Panel also showed that eight out of ten Londoners support the deletion of DNA data of non-convicted individuals.[43] This model is perceived to be proportionate or balanced.[44] The PoFA regime appears to be only partially consistent with these views. The DNA records of most non-convicted individuals are excluded from retention. Though data of individuals arrested/charged with serious offences can be retained, "administrative checkpoints" including the independent OBC have been instituted to ensure that their human rights are adequately protected. This policy could enhance public confidence in the operation of the NDNAD.[44] The new regime could also improve the level of transparency in DNA retention by keeping innocent individuals fully informed when the police request extended retention.

While the PoFA regime would appear to offer a good level of genetic privacy protection for the innocent, the system is in sharp contrast with the health service model of informed consent, which is applied in medical research and the operation of medical biobanks.[45] The extended retention of forensic DNA profiles of individuals arrested/charged with a serious offence takes no regard of the informed consent of the individual, their right to withdraw consent and deletion of data. It appears that the State has more power over these arrestee/charged non-convicted individuals, and indirectly this category of individuals seems to be less "innocent" than other non-convicted individuals or volunteers. This raises the question of the proportionality of the PoFA regime.[15,22]

Another concern with the genetic privacy of individuals is that the new retention policy focuses upon the data of the innocent. Although the DNA profiles of some first time convicted minors are subjected to fixed retention, the bulk of convicted individuals are subjected to indefinite retention. There is no consideration of the seriousness of offence and severity of sentence as emphasised by the ECtHR in *W v The Netherlands*[46] and characteristic of the Dutch system and many others internationally.[47] The PoFA model may be problematic because the stored DNA profile can be used to track biological relatives through familial searching. This means that the family of the individual may be subjected to indefinite bio-surveillance though innocent. Some issues raised are whether individuals have the right to surrender their genetic information to the government along with that of their innocent biological family without their knowledge or informed consent.[23] Further, what assurances are required to ensure

that the privacy of biological relatives is adequately protected. These are vital considerations in establishing a proportionate regime.

The review indicates an improvement in the match output of the NDNAD following PoFA implementation (current match rate of 63.3%). This suggests that, potentially, the database may be representative of the active criminal population and, if adequately utilised, could improve crime detection and case resolution. Nevertheless, given that DNA hits do not always lead to case resolution due to changes in legislation, investigative and prosecutorial problems, and witness or suspect issues,[48] the match rate does not demonstrate the efficacy of the database. Database match/hit outcomes such as the resolution of cold crimes, crime deterrence and reduction of crime, the efficiency of investigations (e.g. through DNA intelligence hits) and prosecution, and conviction rates have been recommended in previous studies as adequate measures of database efficacy.[48,49] In April 2014, a new Recorded Crimes Outcomes Framework was introduced which allows the police in England and Wales to count database hit outcomes. The specific outcome measures include the number of charges/summons, cautions, deceased offenders, PNDs issued, cannabis warnings and community resolutions. Although this framework is a step towards a more detailed understanding of database effectiveness, it is limited in scope and the efficacy metrics suggested in previous studies[48,49] should be considered.

This review shows that the new retention system has accrued some important secondary benefits including decreased cost of DNA sample storage, improvement of retention compliance checks, and opportunity for case review. In 2006, McCartney[50] reviewed the DNA Expansion Programme and highlighted the high financial cost and resourcing required for the operation of the database, which may be detrimental to resourcing other demands upon police. The requirement to destroy millions of DNA samples under the new regime will therefore potentially create an opportunity for reinvestment in other areas of policing. The introduction of DNA sample retention compliance checks is an important approach to scrutinising police and FSP retention practices. This will help identify gaps between law/policy and practice to enhance the continuous development of effective systems. The periodic assessment will also assure the public how retained DNA material is being used, significantly improving transparency, accountability, public confidence and the assurance of genetic privacy protection. The value of compliance checks requires that the OBC is adequately resourced to cover all forces.

While there is provision for criminal case reviews in the UK, this is mainly focused on cases where a miscarriage of justice is suspected and a first appeal has failed.[51] The selection of cases for cold case investigative reviews is also highly dependent on the seriousness of the offence, availability of resources, opportunities to apply new technology and prospects of case progression.[52] These factors inform the prioritisation of cases hence some cases may be overlooked or re-investigation of the cold case may be delayed. The introduction of Biometric Retention Units offers an opportunity for the police to review all cases to identify those that require an extension of biometric data. This means that gaps, shortcomings and opportunities in some cases may be identified early for re-investigation. For example, the BRU of the MPS identified a case where an NFA-ed person should have been prosecuted and convicted based on the available evidence.

4.2 Challenges of the PoFA implementation

The PoFA retention regime is not problem-free. Firstly, there are critical challenges with the configuration of the Police National Computer that drives the retention and deletion of DNA profiles on the NDNAD. The incompatibility of the PNC undermines the goal of achieving a proportionate DNA data retention system. The implication of the current "compromise" system is that the police can potentially manipulate the system to unlawfully retain or delete data of arrestees.[53] There is a need for thorough audit systems for the technology and PNC processes to identify the scale of potential breaches and resolve technical problems.

Secondly, the success of the current retention system is highly dependent on the cooperation of the police. Poor police engagement puts the public at risk since some crimes (that failed to be prevented) may go undetected. Alternatively, the genetic privacy of some individuals may be breached. In 2008,

Fraser[54] reviewed the Scottish retention system, focussing on the temporal retention of DNA data of unconvicted individuals. The review emphasised that an approach to biometric retention that coordinates policies and practices of all relevant stakeholders is crucial to achieving the aims of the law. The current discretionary PoFA system in England and Wales seem to have been developed without taking account of the views of the police or adequate consideration of police investigative or intelligence-gathering practices and principles. This review indicates some police forces are dissatisfied with the transfer of biometric data retention risks from legislators to the police. Also, the new regime places a demand upon police budgets and resources, other policing areas may thus suffer if PoFA is implemented to the letter. Another reason for poor police engagement is potential PoFA awareness or guidance gaps. A thorough appraisal and survey of police perceptions about the current PoFA retention regime are recommended to understand the underlying issues in order to resolve this challenge.

This review indicates a potential challenge with database contamination. Crime scenes can be contaminated by DNA of police officers or crime scene examiners.[55,56] Evidence items may also be contaminated by laboratory analyst's due to improper handling or poor anti-contamination techniques.[55,56] Furthermore, forensic DNA consumables such as cotton swabs may be contaminated by manufacturers as revealed in the famous "Phantom of Heilbronn" case.[57,58] These factors, together with record handling errors, interpretation and transcription of data errors, may contribute to database contamination.[24] One effective strategy to overcome database contamination is the establishment of elimination databases, which can be crosschecked to eliminate unwanted DNA data.[58–61] Another strategy is routine integrity checks of loaded DNA data.[34] The presence of unwanted profiles on the database can mislead the police or delay the resolution of cases.[55] Another crucial consequence is that where a subject profile is matched with wrong arrestee/sampling information, data may be unlawfully retained or deleted under the current PoFA system. Moreover, database contamination can lead to the wrong estimation of database effectiveness output or outcome metrics. The challenge of database contamination is acknowledged in the reports and plans are underway to eradicate contamination and mitigate the risks associated with this issue.

Most of the reports indicate that the governance of the CTDNAD is inadequate. This may be a contributing factor in the emerging issues associated with the complex NSD process. Although the Strategy Board has an oversight function of the CTDNAD, this is mainly focused on the technical, scientific and operational aspects.[35] To maintain transparency, accountability and public confidence in the retention and use of individuals' data, the current governance arrangements for the NDNAD should be applied to the CTDNAD. Information about governance, guidance policies, statistics of profiles held on the database per retention category, the primary (and any secondary) use of individual's data and match rate should be in the public domain. This is crucial because unlike the NDNAD, unconvicted individuals are not informed about the grounds for extended retention of their data through the NSD process.

A key characteristic of the current PoFA system is discretionary retention. This policy introduces a level of subjectivity in deciding when retention of some unconvicted individuals is necessary. There could be biases in the number of cases selected or approved for extended retention. This is problematic because specific guidance and legal definitions are lacking. Although some guidance has been developed by the Biometrics Commissioner and the Strategy Board, this has not been subjected to robust public or Parliamentary debate. Another problem is that the discretionary retention policy appears bureaucratic and expensive to implement – potentially delaying police work. As suggested by the Biometrics Commissioner, it may be worth abolishing the discretionary retention policy and introducing a bright-line rule, which could be more cost-efficient. Another important issue with discretionary retention is the non-consensual resampling of individuals after data deletion (as amended by s144 of ASBCPA). The initial policy of resampling by consent may be more ethical than the current rule. The new rule may have adverse psychological impacts or ethical implications for unconvicted individuals. For example, after an individual has been acquitted of an offence (or an investigation/ prosecution halted), the person should note that compulsory resampling is still open – granting more power to the State over its citizens' genetic property. There is a need for public debate and consultation with relevant agencies to consider the ethical impact of this policy.

The current PoFA regime provides for the destruction of the DNA sample after profiling because of its sensitivity. Under some circumstances, however, the DNA sample of a known individual may be required for prosecution disclosure purposes, which is provided for by the current law (s146 of ASBCPA). The CPIA exception permits the sample to be stored beyond the statutory 6 months' period but it must be destroyed after its purpose has been fulfilled. Sensitive private information such as health and disease risk can be predicted using DNA sequencing technologies.[62,63] This type of analysis requires the original DNA sample and its retention is perceived to be disproportionate and unnecessary in the prevention and detection of crime.[44,64] To maintain public confidence in the temporal retention and proper use of DNA samples, there is a need for transparent and accountable oversight. An effective audit system must be established to prevent the misapplication of the CPIA rule by police forces. Access to retained DNA samples should be restricted to vetted officers and sufficient information about governance, the number of samples held and use should be in the public domain.

The final challenge with PoFA implementation is volunteer sampling and samples. Volunteer DNA data plays a crucial role in investigative work. It can be used to detect contamination or eliminate people who are unlikely to be suspected in a case such as victims, relatives or friends. The sensitivity of the DNA sample calls for restrictive access and adequate protections against misuse. Although new policy guidance consistent with PoFA is being developed, there is a need for clear statutory regulations informed by public debate and consultation with stakeholders. This is important because volunteer data can be subjected to the same treatment as arrestees – including speculative and familial searching.

4.3 Risks and emerging issues

Though there is limited information to justify retention of DNA material of unconvicted individuals, it is known that some individuals within this category may be actual offenders or may commit a crime in the future.[65] This is also true however, for the entire population who are presumed innocent. Preliminary studies by Pease[66] and Tseloni and Pease[67] show subsequent re-arrest and conviction among unconvicted individuals. The re-arrest rate is estimated to be at the same rate as that of individuals cautioned or given non-custodial sentences – approximately 52% within 6 years.[18] While the reliability of this statistic has been questioned,[15] both preliminary studies suggest that discretionary retention of DNA data from unconvicted individuals based on the seriousness of offence or age may diminish crime detection efforts. These conclusions are consistent with the assertion of the Biometrics Commissioner that some crimes may go undetected or fail to be prevented because all arrestee data are not subjected to indefinite retention. These views suggest that the PoFA retention regime may be slightly skewed towards individual privacy rights and there is a need for careful consideration of the competing public interests, especially because extended retention is mainly considered for serious offences. Regarding the ethical issues associated with the re-sampling arrest of individuals with convictions from outside England and Wales, the new Policing and Crime Act 2017[68] permits indefinite retention of material taken from an unrelated arrest. The scope of sampling has also been expanded to include all offences equivalent to a recordable offence under English and Welsh law. These changes are at par with individuals convicted of recordable crimes in England and Wales. It may be safe to assume that the public security risks associated with non-retention of the biometric material of this category of individuals will be mitigated by including their DNA records on the NDNAD.

Another important emerging issue is the contention surrounding the future benefits of retention, particularly for domestic violence offences. There is extant research that establishes the heterogeneity of offences committed by individual offenders.[67,69,70] Though retention may not be beneficial to a domestic offence investigation involving the same victim, retention may be valuable to other offences such as stranger rape. Indirectly, DNA retention may have a "secondary" deterrence effect on the NFA-ed arrestee of a domestic offence.

Clearly, the restrictions of PoFA may limit the intelligence gathering efforts of the police. There should be adequate guidance and statutory rules on the use of unlawful matches to avoid the public security concerns and legal challenges encountered previously under the CJPOA regime (See *R v B, Attorney General's Reference No 3 of 1999 [2000] UKHL 71 (UKHL (2000))* and *R v Weir [2000] EWCA Crim*

43). The question remains, if an unlawful match is obtained and the DNA link is the only evidence that can progress a case, should it be acted upon? What should be the procedure under such circumstances? As pointed out by the Biometrics Commissioner, current police practice may be contrary to the law. However, there may be circumstances whereby an unlawful match may be the only investigative lead in an unsolved crime. These factors should be carefully considered in striking the right balance between public and private interests.

In the Government's response to the 2015 annual report of the Biometrics Commissioner, it was indicated that Parliament would consider a legislative instrument expanding the list of qualifying offences by the end of 2016.[71] It is not clear what other offences may be considered apart from those suggested by the Commissioner. It appears that the opportunity to expand the list may widen the inclusion criteria and facilitate database expansion. It is highly recommended that the core principles and relevant factors applied by the Commissioner including the relevance of DNA and the potential crime reduction or detection value of retention should be considered. Also in the Government's response, it was stated that new guidance would be issued to resolve the issue of retaining DNA data after a match without arrest.

Finally, the review identified limited statutory regulation for "new" genetic technologies that are not specifically covered by PoFA. It appears that Y-STR profiling and databasing are being applied, though under strict regulation, without a dedicated legislation or comprehensive public consultation and debate. In a review of the legislative framework governing the NDNAD and the Netherlands DNA database, Toom[72] concluded that the "Dutch model" of dedicated legislation to genetic technology implementation offers civil rights advantages over the English and Welsh model of technology implementation to "legislative fixes". This is consistent with recent recommendations by the Forensic Genetics Policy Initiative.[44] The inclusion of privacy rules in legislation and from the onset of establishing genetic databases is perceived to be easier than its introduction after establishing the database.[44] To avoid the historical legal challenges associated with the NDNAD, the Dutch model should be considered for new genetic technologies.

5 Conclusion

This paper reviewed a total of ten reports of the two independent statutory authorities (NDNAD Strategy Board and the Office of the Biometrics Commissioner) and an independent non-statutory advisory public body (NDNAD Ethics Group) specifically tasked with oversight of the UK National DNA Database. The purpose of the review was to identify the benefits, challenges, risks and emerging issues associated with the implementation of the new DNA retention regime introduced by the Protection of Freedoms Act 2012. The review indicates that the system may have improved the match output of the database, with a current match rate of 63.3%. Compared to previous regimes, it appears the composition of the database under the PoFA regime may be more representative of the active criminal population and the regime may improve the crime-solving capacity of the database. Additionally, the new system has strengthened the genetic privacy protection of UK citizens, particularly the genetic privacy of the innocent. This benefit may improve public confidence in the operation of the database. The implementation challenges identified ranges from the Police National Computer configuration, legal and procedural issues to sufficient understanding of the requirements of PoFA by police forces. The review shows that some "retainable" profiles have been deleted and this may potentially diminish crime detection or reduction and raise public security concerns. Also, some DNA data have been unlawfully retained and the current police practice permits the use of unlawful matches for intelligence purposes. This policy may lead to privacy issues and challenges in court. Although limited in scope, this review advances the literature on the global evolution of forensic DNA database policy. The review shows that the current law in UK could potentially improve the effectiveness of forensic DNA databases whilst complying with human rights law. The challenges identified, however, suggest that there may be a significant gap between the law and implementation. Overall, the review emphasises the need for comparative empirical research to adequately demonstrate the efficacy of forensic DNA databases. Objective research is vital because this review focused on reports of government bodies and there is a possibility of framing or reporting bias. The crucial areas to consider include the perception of stakeholders directly involved in the operation and use of the database, and the impact of different

retention criteria and retention lengths on the performance of the database. This may help establish adequate public security and human rights standards for the NDNAD and potentially forensic biometric databases worldwide.

Conflict of interest

None declared.

Ethical Approval

This work is part of a doctoral research which has been approved by the Institute's Ethics Committee.

Funding

This work was undertaken as part of the author's PhD in Law at Northumbria University, Newcastle, UK. The doctoral research is funded by a Northumbria University Research Studentship.

References

1. Home Office. National DNA Database statistics, Q2 2017 to 2018 [Internet]. GOV.UK 2017 [cited 2017 Oct 30]; Available from: https://www.gov.uk/government/statistics/national-dna-database-statistics

2. McCartney C. The DNA Expansion Programme and Criminal Investigation. Br J Criminol 2006;46(2):175–92.

3. Bramley B. DNA Databases. In: Fraser J, Williams R, editors. Handbook of forensic science. Cullompton: Willan Publishing; 2009. page 309–36.

4. Williams R, Johnson P. Circuits of Surveillance. Surveill Soc 2004;2(1):1–14.

5. Smith L, Bond J. Criminal Justice and Forensic Science: A Multidisciplinary Introduction. New York: Palgrave Macmillan; 2014.

6. Tolfts L, Keay R. Caught by his lust for call-girls; a chance call about cheque fraud led to police capturing Britain's most wanted serial rapist in the bedroom of this hotel in Rugby [Internet]. Free Libr.1999 [cited 2017 Jan 19]; Available from: https://www.thefreelibrary.com/Caught+by+his+lust+for+call-girls%3B+A+CHANCE+CALL+ABOUT+CHEQUE+FRAUD...-a060456713

7. Williams R, Johnson P. Inclusiveness, Effectiveness and Intrusiveness: Issues in the Developing Uses of DNA Profiling in Support of Criminal Investigations. J Law Med Ethics 2005;33(3):545–58.

8. Gershaw CJ, Schweighardt AJ, Rourke LC, Wallace MM. Forensic utilization of familial searches in DNA databases. Forensic Sci Int Genet 2011;5(1):16–20.

9. Butler J. Advanced topics in forensic DNA typing: methodology. London: Elsevier; 2012.

10. Criminal Justice and Public Order Act [Internet]. 1994 [cited 2016 Oct 9]. Available from: http://www.legislation.gov.uk/ukpga/1994/33/contents

11. R v Weir [Internet]. 2000 [cited 2016 Oct 9]. Available from: http://www.bailii.org/ew/cases/EWCA/Crim/2000/43.html

12. MacGregor A. Annual report 2014: Commissioner for the Retention and Use of Biometric Material [Internet]. Office of the Biometrics Commissioner, UK; 2014 [cited 2016 Oct 11]. Available from: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014

13. McCartney C. Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach. Crit Criminol 2004;12(2):157–78.

14. Simoncelli T, Wallace H. Spiralling Out of Control. Index Censorsh 2005;34(3):55–60.

15. McCartney C. Of Weighty Reasons and Indiscriminate Blankets: The Retention of DNA for Forensic Purposes. Howard J Crim Justice 2012;51(3):245–60.

16. S and Marper v The United Kingdom [Internet]. 2008 [cited 2016 Mar 11]. Available from: http://www.bailii.org/eu/cases/ECHR/2008/1581.html

17. Crime and Security Act [Internet]. 2010 [cited 2016 May 1]. Available from: http://www.legislation.gov.uk/ukpga/2010/17/pdfs/ukpga_20100017_en.pdf

18. Home Office. Keeping the right people on the DNA database: Science and Public Protection. London: Home Office; 2009.

19. Home Office. Protection of Freedoms Act 2012: how DNA and fingerprint evidence is protected in law [Internet]. GOV.UK2013 [cited 2016 Oct 8]; Available from: https://www.gov.uk/government/publications/protection-of-freedoms-act-2012-dna-and-fingerprint-provisions/protection-of-freedoms-act-2012-how-dna-and-fingerprint-evidence-is-protected-in-law

20. Protection of Freedoms Act [Internet]. 2012 [cited 2016 Oct 8]. Available from: http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

21. Home Office, Brokenshire J. Protection of Freedoms Act implementation and National DNA Database annual report 2012 to 2013 [Internet]. GOV.UK2013 [cited 2016 Mar 11]; Available from: https://www.gov.uk/government/speeches/protection-of-freedoms-act-implementation-and-national-dna-database-annual-report-2012-to-2013

22. Blakemore B, Blake C. Can the National DNA Database be Effective and Comply with Human Rights Legislation? Police J 2012;85(3):191–202.

23. Lee J. The presence and future of the use of DNA-Information and the protection of genetic informational privacy: A comparative perspective. Int J Law Crime Justice 2016;44:212–29.

24. National DNA Database Strategy Board. National DNA Database: annual report, 2015 to 2016 [Internet]. National DNA Database Strategy Board, UK; 2017 [cited 2017 Feb 27]. Available from: https://www.gov.uk/government/publications/national-dna-database-annual-report-2015-to-2016

25. Wiles P. Annual Report 2016: Commissioner for the Retention and Use of Biometric Material [Internet]. Office of the Biometrics Commissioner, UK; 2017. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644755/CCS207_CCS0917991760-1_Biometrics_Commissioner_ARA_Accessible.pdf

26. National DNA Database Ethics Group. Annual report of the Ethics Group: National DNA Database 2015 [Internet]. UK: National DNA Database Ethics Group; 2016 [cited 2017 Feb 16]. Available from: https://www.gov.uk/government/publications/national-dna-database-ethics-group-annual-report-2015

27. Home Office. Biometrics and Forensics Ethics Group Terms of Reference, Code of Practice & Working Protocol [Internet]. 2017 [cited 2017 Oct 26]; Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636963/BFEG_-_Terms_of_Reference_Code_of_Practice_and_Working_Protocol_-_4_April_2017.pdf

28. MacGregor A. Annual report 2015: Commissioner for the Retention and Use of Biometric Material [Internet]. Office of the Biometrics Commissioner, UK; 2016 [cited 2016 Oct 11]. Available from: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2014-to-2015

29. Nicholson E, Murphy T, Larkin P, Normand C, Guerin S. Protocol for a thematic synthesis to identify key themes and messages from a palliative care research network. BMC Res Notes 2016;9.

30. Ryan G, Bernard H. Techniques to Identify Themes. Field Methods 2003;15:85–109.

31. Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol 2006;3(2):77–101.

32. Javadi M, Zarea K. Understanding Thematic Analysis and its Pitfall. J Client Care 2016;1(1):33–9.

33. National DNA Database Strategy Board. National DNA Database: annual report, 2013 to 2014 [Internet]. National DNA Database Strategy Board, UK; 2014 [cited 2017 Feb 16]. Available from: https://www.gov.uk/government/publications/national-dna-database-annual-report-2013-to-2014

34. National DNA Database Strategy Board. National DNA Database: annual report, 2014 to 2015 [Internet]. National DNA Database Strategy Board, UK; 2015 [cited 2016 Mar 11]. Available from: https://www.gov.uk/government/publications/national-dna-database-annual-report-2014-to-2015

35. National DNA Database Ethics Group. Annual report of the Ethics Group: National DNA Database 2014 [Internet]. UK: National DNA Database Ethics Group; 2015 [cited 2017 Feb 16]. Available from: https://www.gov.uk/government/publications/ndnad-ethics-group-7th-annual-report-2015

36. National DNA Database Ethics Group. Annual report of the Ethics Group: National DNA Database 2016 [Internet]. UK: National DNA Database Ethics Group; 2017 [cited 2017 Nov 7]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655881/Annex_C_EG_Annual_Report_2016.pdf

37. MacGregor A. Further report by the Biometrics Commissioner on issues raised in his 2015 annual report [Internet]. Office of the Biometrics Commissioner, UK; 2016 [cited 2017 Feb 16]. Available from: https://www.gov.uk/government/publications/biometrics-commissioners-annual-report-2015-further-report

38. Biometrics Commissioner. Consultation Paper on Applications to the Biometrics Commissioner under s.63G PACE Summary of Responses [Internet]. UK: Office of the Biometrics Commissioner; 2013 [cited 2017 Oct 31]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261625/PACE_responses.pdf

39. McCartney C, Wilson TJ, Williams R. Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability. Eur J Crim Policy Res 2011;17(4):305–22.

40. McCartney C. Forensic data exchange: ensuring integrity. Aust J Forensic Sci 2014;47(1):36–48.

41. Sallavaci O. Cross border exchange of forensic DNA and human rights protection. Forensic Sci Int Genet Suppl Ser 2015;5:e86–8.

42. Wallace H, Jackson AR, Gruber J, Thibedeau AD. Forensic DNA databases–Ethical and legal standards: A global review. Egypt J Forensic Sci 2014;4(3):57–63.

43. MPA Civil Liberties Panel. Protecting the innocent: The London experience of DNA and the National DNA Database [Internet]. London: Metropolitan Police Authority; 2011 [cited 2017 Mar 29]. Available from: http://policeauthority.org/metropolitan/downloads/scrutinites/dna.pdf

44. FGPI. Establishing best practice for forensic DNA databases [Internet]. Forensic Genetics Policy Initiative; 2017 [cited 2017 Oct 3]. Available from: http://dnapolicyinitiative.org/wp-content/uploads/2017/08/BestPractice-Report-plus-cover-final.pdf

45. Levitt M. Forensic databases: benefits and ethical and social costs. Br Med Bull 2007;83(1):235–48.

46. W v The Netherlands [2009] (ECHR). Application No. 20689/08

47. Vervaele JAE, Graaf FCW de, Tielemans N. The Dutch Focus on DNA in the Criminal Justice System: Net-widening of Judicial Data. Rev Int Droit Pénal 2013;Vol. 83(3):459–80.

48. Bieber FR. Turning Base Hits into Earned Runs: Improving the Effectiveness of Forensic DNA Data Bank Programs. J Law Med Ethics 2006;34(2):222–33.

49. Gabriel M, Boland C, Holt C. Beyond the cold hit: measuring the impact of the national DNA data bank on public safety at the city and county level. J Law Med Ethics 2010;38(2):396–411.

50. McCartney C. Forensic Identification and Criminal Justice: Forensic science, justice and risk. Cullompton: Willan Publishing; 2006.

51. CCRC. Who we are [Internet]. Crim. Cases Rev. Comm. [cited 2017 Mar 14];Available from: http://www.ccrc.gov.uk/about-us/who-we-are/

52. Fraser J. Cold-Case Review: UK Experience. In: Encyclopedia of Forensic and Legal Medicine (Second Edition). Oxford: Elsevier; 2016. page 576–80.

53. Martin A. Cops hacked the Police National Computer to unlawfully retain suspects' biometric data [Internet]. The Register2016 [cited 2017 Mar 14]; Available from: https://www.theregister.co.uk/2016/03/14/cops_hack_police_national_computer_unlawfully_retain_biometric_data/

54. Fraser J, Scottish Government (Funder). Acquisition and retention of DNA and fingerprint data in Scotland [Internet]. University of Strathclyde; 2009 [cited 2016 Oct 11]. Available from: http://strathprints.strath.ac.uk/18671/

55. Forensic Science Regulator. DNA contamination detection -The management and use of staff elimination DNA databases [Internet]. Birmingham: Forensic Science Regulator; 2014 [cited 2017 Aug 31]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/355995/DNAcontaminationDetection.pdf

56. Forensic Science Regulator. The Control and Avoidance of Contamination in Crime Scene Examination involving DNA Evidence Recovery [Internet]. UK: Forensic Science Regulator; 2016. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536827/FSR-anti-contamination.pdf

57. Neuhuber F, Dunkelmann B, Höckner G, Kiesslich J, Klausriegler E, Radacher M. Female criminals—It's not always the offender! Forensic Sci Int Genet Suppl Ser 2009;2(1):145–6.

58. Lapointe M, Rogic A, Bourgoin S, Jolicoeur C, Séguin D. Leading-edge forensic DNA analyses and the necessity of including crime scene investigators, police officers and technicians in a DNA elimination database. Forensic Sci Int Genet 2015;19:50–5.

59. Pickrahn I, Kreindl G, Müller E, Dunkelmann B, Zahrer W, Cemper-Kiesslich J, et al. Contamination when collecting trace evidence—An issue more relevant than ever? Forensic Sci Int Genet Suppl Ser 2015;5:e603–4.

60. Sullivan K, Johnson P, Rowlands D, Allen H. New Developments and Challenges in the Use of the UK DNA Database: Addressing the Issue of Contaminated Consumables. Mediterr Acad Forensic Sci 1st Workshop 2004;146, Supplement:S175–6.

61. Fonneløp AE, Johannessen H, Egeland T, Gill P. Contamination during criminal investigation: Detecting police contamination and secondary DNA transfer from evidence bags. Forensic Sci Int Genet 2016;23:121–9.

62. Lehrach H. DNA sequencing methods in human genetics and disease research. F1000Prime Rep 2013;5(34).

63. Børsting C, Morling N. Next generation sequencing and its applications in forensic genetics. Forensic Sci Int Genet 2015;18(Supplement C):78–89.

64. Krimsky S, Simoncelli T. Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties. New York: Columbia University Press; 2011.

65. Wallace H. The UK National DNA Database: Balancing crime detection, human rights and privacy. EMBO Rep 2006;7(Spec No):S26–30.

66. Pease K. DNA retention after S and Marper. In: Keeping the right people on the DNA database: Science and Public Protection. London: Home Office; 2009.

67. Tseloni A, Pease K. DNA Retention after Arrest: Balancing Privacy Interests and Public Protection. Eur J Criminol 2011;8:32–47.

68. Policing and Crime Act [Internet]. 2017 [cited 2017 Mar 17]. Available from: http://www.legislation.gov.uk/ukpga/2017/3/contents/enacted

69. Leary D, Pease K. DNA and the Active Criminal Population. Crime Prev Community Saf 2003;5(1):7–12.

70. Townsley M, Smith C, Pease K. Using DNA to catch offenders quicker: serious detections arising from criminal justice samples. Genomics Soc Policy 2006;2(1):28–40.

71. Lewis B. Response to the Biometrics Commissioner's annual report 2015 [Internet]. 2016 [cited 2017 Mar 16]; Available from: https://www.gov.uk/government/publications/response-to-the-biometrics-commissioners-annual-report-2015

72. Toom V. Forensic DNA databases in England and the Netherlands: governance, structure and performance compared. New Genet Soc 2012;31(3):311–22.

Table 1 – Summary of the different legislative regimes enacted/proposed to govern DNA profile retention on the England and Wales NDNAD

Retention category		**Criminal Justice and Public Order Act 1994 (*Restrictive regime*)**	**Criminal Justice and Police Act 2001 & Criminal Justice Act 2003 *(Expansive regime)***	**Crime and Security Act 2010 (Repealed)**	**Protection of Freedoms Act 2012 *(semi-restrictive regime)***
CONVICTION					
Adults	All crimes	Indefinite	Indefinite	Indefinite	Indefinite
Under 18 years	Serious offence			Indefinite	Indefinite
	Minor Offence			*First conviction:* 5 years *Second conviction:* indefinite	*First conviction:* 5 years + length of sentence *Second conviction or custodial sentence > 5 years:* indefinite
NON-CONVICTIONS					
All offences		Automatic deletion after conclusion of investigation or proceedings [α]	Indefinite	*Adults:* 6 years *Under 18 years*: 3 years	Automatic deletion after conclusion of investigation or proceedings
Charged with a Qualifying Offence					3 years (2-year renewal with consent of District Judge)
Arrested for a qualifying offence					3 years may be granted by Biometrics Commissioner (2-year renewal with consent of District Judge)
Issued with a Penalty Notice for Disorder (PND)					2 years
Terrorist suspects		Indefinite [β]		6 years (+possible multiple 2 years with National Security Determination (NSD) by Chief Constable)	Retention under relevant legislation [γ] (+ possible multiple 2 years with NSD by Chief Constable)

(NB: [α]Samples/profiles of the innocent could be retained if the individual is part of a group of suspects of whom at least one was convicted in the relevant case. The retained material, however, could not be used as evidence against the individual or for investigation purposes. [β]No obligation to destroy data under Prevention of Terrorism Act 1989. [γ] Including Terrorism Act 2000, Counter-terrorism Act 2008, Terrorism Prevention and Investigation Measures Act 2011)

Table 2 – Selected annual or official reports included in review

Body	Report Title	Period	Date Published
National DNA Database Strategy Board	National DNA Database: annual report 2013-14[33]	2013-2014	16/12/2014
	National DNA Database: Annual Report 2014/15[34]	2014-2015	14/12/2015
	National DNA Database: Annual report 2015/16[24]	2015-2016	23/02/2017
National DNA Database Ethics Group	Annual report of The Ethics Group: National DNA Database 2014[35]	2014	24/03/2015
	Annual report of The Ethics Group: National DNA Database 2015[26]	2015	16/11/2016
	Annual report of the Ethics Group: National DNA Database 2016[36]	2016	30/10/2017
Office of the Biometric Commissioner	Annual report 2014: Commissioner for the Retention and Use of Biometric Material[12]	2013-2014	16/12/2014
	Annual Report 2015: Commissioner for the Retention and Use of Biometric Material[28]	2014-2015	11/03/2016
	Further Report by The Biometrics Commissioner on Issues Raised in His 2015 Annual Report[37]	2014-2015	26/05/2016
	Annual Report 2016: Commissioner for the Retention and Use of Biometric Material[25]	2015-2016	13/09/2017

Table 3 – Main themes identified from the reviewed reports

Category	**Themes**	**Number of reports**
Benefits of PoFA	Improved, proportionate balance between public and private interests	9
	Increased match rate	7
	Decreased sample storage cost	1
	Strengthened retention compliance checks	3
	Opportunity for case review	3
Challenges of PoFA implementation	Police National Computer (PNC) limitations	3
	Non-engagement of police forces with PoFA	3
	Limited data on case resolution rate	9
	Database contamination and error rates	7
	Inadequate enforcement of PoFA rules for Counter-terrorism DNA Database (CTDNAD)	6
	Limited statutory guidance on discretionary retention	5
	Misapplication of Criminal Procedure and Investigations Act 1996 (CPIA) exception	3
	Inadequate rules for volunteer sampling and samples	6
Risks/emerging issues associated with PoFA implementation	Public security risk due to non-retention of data	3
	Breach of privacy due to unlawful retention	4
	Contention surrounding future benefits of retention	3
	Need for expansion of qualifying offences	3
	Retention after a match but without arrest	3
	Complex National Security Determination (NSD) process	4
	Resource needs for compliance checks	3
	Limited statutory guidance for new genetic technologies	3