Privacy Commissioner's Submission to the Law Commission on the Use of DNA in Criminal Investigations (Issues Paper 43)

1. Introduction

1.1. I welcome the Law Commission's Issues Paper 43 and its review of the Criminal Investigations (Bodily Samples) Act 1995 (the CIBS Act). The DNA databanks have important law enforcement purposes. However, it is timely to assess the CIBS Act to ensure it is made fit for purpose.

1.2. Collecting, analysing and retaining individuals' DNA raises important privacy considerations especially in a law enforcement context. Clear legislative parameters and appropriate checks and safeguards are necessary to ensure that intrusions into the privacy of the individual are not unwarranted, and to limit any unintended adverse effects for individuals.

1.3. The significant privacy implications have been noted by senior judges and law officers, as well as current and former Privacy Commissioners.

1.4. Winkelmann J (now Chief Justice) encapsulated the relationship between privacy, dignity and autonomy in a public lecture last year:[1]

> *… the ability to keep private our bodies by maintaining control over them, and to keep private information about ourselves, is essential to human dignity, and the related value, the autonomy of the person. An invasion of privacy which undermines or negates that dignity can be profoundly harmful for the individual. It can distress, humiliate and shame. In extreme cases it can destroy the social and economic foundations of an individual's life.*

1.5. The Attorney-General's report on the 2009 amendment to the CIBS Act noted that: [2]

> *The taking of DNA samples is, both by virtue of the collection process … and the intimate character of genetic information, properly regarded as an invasive search of the person.*

1.6. In a case in the Court of Appeal concerning the taking of a bodily sample under the CIBS Act, Harrison J observed:[3]

> *…it is trite that DNA is not a mere fingerprint: it contains a wealth of genetic information about a person with unlimited future utility. The one-off intrusion of the procedure thus permanently erodes Mr Toki's privacy and freedom, which would usually remain beyond the reach of the state apparatus. Without Mr Toki's informed consent, the bodily sample*

---

[1] Sir Bruce Slane Memorial Privacy Lecture, November 2018.
[2] Hon Christopher Finlayson QC, Report of the Attorney-General under the New Zealand Bill of Rights Act on the Criminal Investigations (Bodily Samples) Amendment Bill https://www.justice.govt.nz/assets/Documents/Publications/BORA-Criminal-Investigations-Bodily-Samples-Amendment-Bill.pdf
[3] *R v Toki* [2018] 2 NZLR 362 at [24].

now stored on the DNA profile databank was obtained in serious, permanent and ongoing breach of his rights.

1.7. Former Privacy Commissioner Marie Shroff submitted to the Select Committee considering the 2009 amendment Bill:[4]

The holding of samples and profiles relating to innocent people on a criminal DNA databank, except when there are compelling law enforcement justifications, concerns me greatly. The databank of DNA information about criminals, gathered and used for law enforcement purposes, must not become by a gradual process a databank of information about the general population.

1.8. The Law Commission's review is an opportunity to address outstanding issues and to strengthen the substantive and procedural safeguards, while ensuring that Police have appropriate access to DNA to support investigations of sufficiently serious criminal offending.

1.9. The Search and Surveillance Act 2012 has modernised a range of law enforcement search powers and applied checks and balances.[5] Law enforcement powers to collect and analyse genetic material similarly warrant attention. The Court of Appeal describes the process as enabling the state to conduct ongoing surveillance of an individual's behaviour "with molecular precision".[6]

1.10. An important reform in my view is to affirm in statute that an individual's genetic material (DNA) is "personal information" (as defined in the Privacy Act). This is necessary to ensure that the privacy principles underpin the collection, analysis use and disclosure of DNA samples, as well as the DNA profiles derived from them.

1.11. In this submission I comment on some of the key privacy issues and provide my initial views on some of the questions arising. I will continue to provide input through my Office's ongoing engagement with this review and am pleased to be represented on the Law Commission's expert advisory group.

Support for reform of the CIBS Act

1.12. I support the two key proposals that the CIBS Act should be replaced, and that there should be independent oversight of the operation and use of the DNA databanks.

1.13. The Issues Paper explains that previous statutory amendments and the developing forensic science have placed pressure on the framework of the Act, and raises important

---

[4] Submission to the Justice and Electoral Committee on the Criminal Investigations (Bodily Samples) Amendment Bill (6 April 2009).
[5] In section 5, the purpose of the Search and Surveillance Act specifically recognises the importance of rights and entitlements affirmed in NZBORA, the Privacy Act and the Evidence Act.
[6] *R v Toki* [2017] NZCA 513, [23].

questions about its fitness for purpose. I am concerned at the Law Commission's findings that the purpose of the CIBS Act is unclear[7] and that it is full of uncertainty.[8]

1.14. Noting that the Issues Paper identifies seven fundamental systemic problems with the CIBS Act (including privacy concerns), and that the regulation provided is partial and not comprehensive, [9] I agree with the conclusion that a new Act is necessary.

1.15. New Zealand needs a comprehensive framework to govern the use of DNA in criminal investigations with a clear purpose statement, and ensure effective governance and oversight. Robust procedural checks and safeguards are necessary so that the DNA databanks are maintained in a manner that ensures the use of DNA in criminal proceedings is necessary, justifiable, reasonable and proportionate.

1.16. It is a fundamental weakness that the original purpose of the CIBS Act has been blurred and that the policy rationale for the collection and retention of DNA for investigative purposes is no longer clear.[10]

1.17. A clear purpose statement is a necessary underpinning for the legislation as a test for decision making and to inform the design of the relevant safeguards. For example, the collection, use, disclosure and retention of personal information (as reflected in the privacy principles) all hinge on an expressly articulated statement of purpose.

1.18. In my view, a legitimate reason needs to be articulated for the State to collect and retain the DNA profiles of some people and not others. The incremental changes to the CIBS Act implemented over time mean there is a risk is that the scheme has become a de facto databank of those citizens who have come to the attention of the Police for a variety of reasons (where through being charged with an offence, being excluded as a suspect, being present in crime scene DNA analysis, or as a victim).

1.19. Function creep can intensify privacy intrusions and erode trust and confidence. Without proper safeguards there is a clear risk of gradual "creep" if DNA gathered for one law enforcement purpose ends up being used for a broader range of purposes than originally articulated or intended.

1.20. There appears to be a real risk of discriminatory impacts. As the Issues Paper notes, this has significant implications for Māori who are over-represented in the justice system. The DNA held in the databank is an available source for the investigation of future offences, regardless of the purpose for which it was originally collected.

---

[7] Executive Summary, para 24.
[8] Issues Paper at [2.34].
[9] Issues Paper, chapter 4.
[10] Issues Paper at [24].

1.21. Some of the Act's weaknesses have previously been raised. In 2009, the former Privacy Commissioner recommended additional safeguards in the legislation.[11]

1.22. The Attorney-General's report under s 7 of the New Zealand Bill of Rights Act identified that the 2009 amendment to the CIBS Act is inconsistent with s 21 of NZBORA.

The Bill provides Police with the power to take DNA databank samples from persons charged with a broad range of offences and, from 2011, any imprisonable offence. As such, the power proposed by the Bill represents a substantial expansion of the current scheme under which such samples are taken only from certain convicted offenders.

….

I have carefully considered whether the power can be regarded as justified and therefore reasonable in terms of s 21. I note, particularly that the propos[al] will very likely result in increased rates of identification and prosecution of offender[s]. However and noting that many comparable jurisdictions operate DNA Databank schemes within these safeguards and the lack of any special circumstances in New Zealand to justify a different approach, it is not possible to conclude that there is a sufficient rationale for their omission here. Further, and given the lack of any statutory constraint, I do not consider that the proposal that Police develop internal guidelines for the exercise of these powers or the possibility that the powers will be interpreted restrictively by the courts provides a sufficiently clear or reliable substitute for statutory safeguards.

The core law reform objectives

1.23. I support the three overlapping core objectives for reform that the Act must be made fit for purpose, constitutionally sound and appropriately accessible.

1.24. Accessibility is necessary to ensure that the framework is transparent, limits the risk of error in its application, and ensures that individuals can access their rights to challenge an erroneous action or decision taken.

1.25. Fitness for purpose in this context must extend to incorporating the necessary safeguards to limit unnecessary intrusion into privacy, dignity, autonomy and other fundamental rights.

1.26. The Legislation Guidelines explain fitness for purpose as providing certainty as to rights and obligations as well as sufficient flexibility to be enduring, but as the Issues Paper notes these are competing factors. Care will be needed here to ensure that flexibility

[11] First, the expansion of collection of samples from people not convicted of an offence without prior external approval should be balanced by appropriate oversight. Second, the extension of collection from all persons charged (but not necessarily convicted) of an imprisonable offence is too low a threshold to be justified. Third, the automatic retention of samples from innocent people is excessive and disproportionate. https://www.privacy.org.nz/news-and-publications/reports-to-parliament-and-government/submissions-on-criminal-investigations-bodily-samples-amendment-bill/.

does not come at a cost to clarity and certainty. The proposed introduction of oversight mechanisms will require sufficient legislative certainty to be effective.[12]

1.27. The Issues Paper appropriately assesses the CIBS Act against important rights, principles and values including the information privacy principles, the principles of the Treaty of Waitangi and values of tikanga Māori, noting the goals of Te Mana Raraunga (the Māori Data Sovereignty network) and Te Ara Tika - guidelines for Māori Research Ethics. These principles overlap and are mutually supporting. A central tenet of both tikanga and human rights (including privacy) is the inherent dignity of all individuals.[13]

1.28. The explanation from a tikanga perspective that it is important there are good reasons for a State intrusion into tapu, including bodily samples, and that those affected understand what is happening and why[14] reflects comparable privacy concepts. For example, the collection of personal information from an individual should be accompanied by a meaningful explanation, and intrusions into personal privacy must be proportionate and justifiable.

1.29. When considering constitutional soundness, it is essential to take account of the right to privacy to inform the nature and design of those safeguards with reference to important and relevant concepts such as necessity, proportionality, and the principle of minimum intrusion.[15]

1.30. The Privacy Act's information privacy principles help to assess the soundness of the CIBS Act and to identify and diagnose how the statute infringes on rights and values that are important to New Zealanders, and how any necessary mitigations can be designed. That includes robust checks and balances in the framework, including the necessary substantive and procedural safeguards.

1.31. In some areas, it will likely be necessary to design more specific safeguards than those provided by the generic privacy principles. Where that is the case, any more specific statutory provision in the CIBS Act can override the relevant privacy principle.[16]

2. Forensic DNA phenotyping (chapter 6)

2.1. DNA phenotyping is a form of predictive modelling – it analyses a person's DNA to predict their likely physical appearance. Predictive modelling raises privacy issues and

[12] Statutes such as the Search and Surveillance Act and Evidence Act have inbuilt periodic review mechanisms. The CIBS Act may be another suitable candidate for periodic review, to allow for any necessary adjustments to be made over time.
[13] Issues Paper at [2.53].
[14] Issues Paper at [2.51(a)].
[15] Issues Paper at [2.84].
[16] Privacy Act 1993, s 7.

was the subject of my keynote speech to last year's Privacy Forum,[17] that discussed the principles for data analytics developed by my Office in conjunction with Statistics NZ.[18]

2.2. I support broad public consultation about regulating DNA phenotyping in any new Act, noting there is potential for discriminatory impacts and that in some jurisdictions the practice has been banned.

2.3. The Issues Paper notes the widespread concerns about the accuracy and utility of forensic DNA phenotyping.[19] Care must be taken to assess the circumstances in which this process can be relied on, and the design of appropriate safeguards. If information derived from phenotyping cannot be relied on as having sufficient accuracy for the purpose for which it is proposed to be used, this may indicate the technique is not fit for purpose.

2.4. One of the key concerns from a privacy perspective is whether the predictive practice is sufficiently accurate to meet the requirements of privacy principle 8. That principle requires an agency such as the Police to ensure that personal information is not used without taking the necessary steps to ensure that it is sufficiently accurate, up to date, complete, relevant, and not misleading, having regard to the purpose for which the information is proposed to be used.

2.5. Given the low incidence of DNA phenotyping in New Zealand (11 instances of ethnic inferencing since 2007), and the significance of the issues it raises, the safeguard of judicial pre-approval may be warranted, as the Law Commission is considering.[20]

The definition of personal information

2.6. The Privacy Act's definition of "personal information" is necessarily broad. Whether information constitutes personal information is a question of fact and context is all important. I agree with the conclusion that information is "identifiable" if it can be used alongside other information to identify a person[21] and support the view that the analysis of crime scene samples will generally be "personal information".

2.7. The CIBS Act should affirm that any information derived from a bodily sample is to be treated as "personal information" as defined in the Privacy Act. While there may be cases where the data is not of sufficient quality or reliability to enable a person to be identifiable,

---

[17] Privacy Commissioner's keynote speech, Privacy Forum (9 May 2018) https://www.privacy.org.nz/assets/Uploads/Privacy-Commissioner-Privacy-Forum-keynote-speech.pdf
[18] May 2018, https://www.privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/.
[19] Issues Paper at [6.71].
[20] Issues Paper at [6.87(a)].
[21] Issues Paper at [6.50].

as a policy matter it is appropriate to treat any information derived from a bodily sample as "personal information", as well as the genetic sample itself.

3. Forensic comparisons (chapter 7)

3.1. This chapter asks about the limits that should apply to the amount of information included in a DNA profile for direct forensic comparison purposes.

3.2. As the Issues Paper notes, privacy principle 1 articulates the fundamental principle that personal information should only be collected to the extent that it is necessary for a lawful purpose. The fact that additional information can now be generated more easily and cheaply does not obviate the need for a clear law enforcement justification for more extensive analysis on a routine basis.

4. Reference Samples – direct collection (chapter 8)

4.1. This chapter outlines the framework for collecting DNA samples directly from an individual by force or by consent.

4.2. If a variety of sample methods is retained, there should be a presumption that the least intrusive option would be used in the circumstances unless there is a justification for departing from that presumption.[22]

4.3. I note the Law Commission is considering three policy options for safeguards for the use of force to obtain a sample.[23] If the power to obtain a sample by force is retained, I agree that the current judicial safeguards should be retained.

4.4. In relation to collection by consent, I support additional safeguards in relation to vulnerable individuals such as children and young people, particularly children in need of care and protection, and individuals of limited decision-making capacity or agency.

4.5. I support the inclusion of statutory protections around the use of elimination samples. An important privacy safeguard is not retaining elimination samples and related DNA profiles for longer than necessary, once the sample and profile are no longer required.[24] Where elimination samples and profiles are retained, there should be clear limits on their use beyond the particular investigation for which they were obtained.

4.6. I note the Law Commission is considering a number of options including review of any match with a crime scene sample. If such matches are likely to be rare, it may be

[22] Issues Paper, Q12.
[23] Issues Paper [8.54]-[8.61].
[24] The current retention period is 24 months (or longer) until any court proceeding is concluded – Issues Paper – table 2, p 308.

appropriate for review to be carried out by a judicial officer who could give directions as to its use, or more generally in relation to practice in the collection of elimination samples.

4.7. I also support the proposal to regulate mass screenings and to put this form of surveillance on a statutory footing.

5. Reference Samples - indirect collection (chapter 9)

5.1. Indirect suspect sampling is where a biological sample is obtained from a secondary source such as a discarded item, rather than directly from the individual concerned. Other secondary sources of generic material include close relatives of the suspect, and genetic samples held for other purposes such as the bloodspot cards collected for the Newborn Metabolic Screening Programme.

5.2. Indirect collection raises important privacy considerations. I agree that a person has a privacy interest in their biological material, no matter where it is found.

5.3. As the Issues Paper notes, privacy principle 2 requires that personal information is collected directly from the individual concerned. Exceptions to this principle relevantly include where non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.[25]

5.4. The Issues Paper suggests it may be appropriate for the Privacy Commissioner to have an auditing role to ensure that indirect suspect sampling is only undertaken in cases where it is justified or reporting obligations could be included in new legislation and trends monitored by an oversight body.[26]

5.5. Accountability for indirect sampling is important, including to verify this meets the necessary threshold for the relevant privacy principle exception. The decision to undertake indirect sampling and the reasons for it should be recorded for audit purposes.

5.6. An alternative option to audit by an oversight body would be for a regular audit to be carried by the Police and/or ESR under a statutory requirement or on a basis agreed with the oversight body.[27] Either IPCA or my Office could receive the results of an audit and consult with the other (and any other relevant stakeholders) on any particular trends

[25] IPP 2(2)(d).
[26] Issues Paper at [9.75].
[27] Agency audits are a feature of the Privacy Act's Part 9A information sharing regime, and as provided for in the reporting requirements of the Privacy Regulations 1993. See also the requirements for direct access agreements in the Intelligence and Security Act 2017, s 126(b).

or issues arising. The oversight bodies could then make further inquiries and public comment about the results and any issues arising.

Bloodspot cards

5.7. In relation to the Newborn Metabolic Screening Programme, the Health Information Privacy Code (HIPC), Schedule 3 issued as a form of legislative instrument under the Privacy Act, [28] is relevant in controlling the purposes for which the blood spot cards may be used.[29] I support consideration of whether these controls should now become part of a statutory regime.

5.8. The Issues Paper notes remaining concerns about the use of search warrants to access blood spot cards (that override the controls that otherwise apply).

5.9. If there is a demonstrable law enforcement need to access blood spot cards in rare circumstances by search warrant, one option is to create conditions or limits on the issue of these warrants, to reflect the intent that they are to be used as a last resort in necessary circumstances (as reflected in the MOU). However, the potential use of warrants should be carefully balanced against the potential impact on the screening programme.

5.10. In the absence of an adequate policy rationale for accessing bloodspot cards by search warrant, an alternative is to restrict their use for law enforcement purposes as set out in the HIPC (and remove the search warrant as a permitted secondary purpose).[30]

Genealogical websites

5.11. I note that the Police has not and is not considering the use of genetic information available from consumer genealogical websites.[31]

5.12. This practice gives rise to significant privacy concerns including the use of genetic data voluntarily provided for one purpose, for a very different purpose. [32] Nor is it necessarily

---

[28] Privacy Act 1993, s 50.
[29] https://www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/Consolidated-HIPC-current-as-of-28-Sept-17.pdf
[30] Health Information Privacy Code 1994, Schedule 3, "permitted secondary purpose" para (d).
[31] Issues Paper at [9.119].
[32] On privacy issues arising in consumer generic testing, see the work of Dr Andelka Phillips, http://www.andelkamphillips.com/ a speaker at OPC's International Privacy Forum (4 December 2018) https://www.privacy.org.nz/forums-and-seminars/international-forums/international-privacy-forum/

subject to the scientific method and storage protocols that operate in our criminal justice context to provide appropriate oversight of chain of custody.

5.13. In my view, a precautionary principle to the potential use of commercialised DNA analysis should operate and access by law enforcement should be statutorily limited or controlled in any new legislation.

6. Crime Sample Databank (chapter 10)

6.1. I support a seriousness threshold being considered for the uploading of crime scene profiles, and the reform of the Crime Sample Databank. I note the identified issues of concern including retention and a lack of safeguards, and I support greater protections in relation to the use of victim (and potentially third party) profiles.

6.2. It is notable that other jurisdictions have adopted a crime scene index in legislation that provides rules on matching within and between indices. Importantly, this approach allows for controls on subsequent access to and use of DNA information to be embedded. This is consistent with the Privacy Act's discipline and controls on data matching in the public sector more generally.[33]

6.3. Low quality crime scene profiles raise potential issues under privacy principle 8. I suggest that consideration be given to whether such samples must meet a certain quality to be eligible for uploading to the Crime Scene Databank or whether they should be tagged as being of low quality so that additional checks can be undertaken before such samples are used or relied on for investigative purposes.

6.4. The paper raises issues in relation to reporting and the lack of good data to measure effectiveness. I agree this is an important dimension to accountability and oversight. As a point of comparison, Part 9A of the Privacy Act includes provision for agency reporting on information sharing initiatives.[34]

7. Known person databank – collection (chapter 11)

7.1. When the CIBS Act was enacted, the first Privacy Commissioner, the late Sir Bruce Slane was concerned about the scope of the discretion to collect samples by consent being wider than necessary to meet the law enforcement objectives.[35] In light of the Law Commission's finding that few databank consent samples are now obtained, it would be timely to review whether this method of collection should be retained.

7.2. There is a real question about whether the discretionary power to collect DNA samples by consent for the known person databank (from persons other than suspects or

---

[33] Privacy Act 1993, Part 10, Schedule 4.
[34] Privacy Act 1993, s 96T, Privacy Regulations 1993.
[35] Report by the Privacy Commissioner to the Minister of Justice on the Criminal Investigations (Blood Samples) Bill (20 February 1995).

convicted offenders) is too broad to protect individuals from the risk of inadvertent bias or discriminatory targeting.

7.3. The threshold for obtaining DNA profiles for the known person databank should be set at an appropriate level of seriousness. The breadth of the current list of triggering offences (any imprisonable offence) does not appear to be proportionate.

7.4. A set of protocols or controls should be designed that reflect the underlying purpose of the databank. These controls could restrict the use of a sample depending on the timing of collection (whether before or after conviction), the purpose of collection (whether a suspect sample or on arrest or conviction) and could apply different retention periods, for example using indices.

8. Known person databank – use (chapter 12)

8.1. This chapter asks about the appropriate limits on sharing information from the NZ databanks with overseas foreign law enforcement, including familial searches. It is important to ensure that the legislative settings for international information sharing align with those set domestically and are not more permissive.

8.2. In relation to research uses, the sensitivity of the databanks suggests that a framework for ethics approvals should be considered that incorporates meaningful consultation with representative groups, including Māori.

8.3. This chapter also discusses potential personal uses of the DNA databank. I suggest that familial access rights should be further considered in the Law Commission's deliberations.

8.4. The CIBS Act affirms rights of access to information in the databank to the person to whom the information relates in accordance with the Privacy Act. A number of different people may have an interest in the genetic information of an individual represented in the databank and may in some circumstances have a legitimate reason to seek access to it.

8.5. A relative of a person whose DNA profile is stored on the databank could seek access to that information (for example to test for a life threatening inherited genetic condition) on the basis that it is personal information about the requester (as well as the person the profile directly relates to). It may not be necessary for the individual seeking access to provide their own DNA sample (as the Issues Paper suggests) to prove connection[36] – that could be confirmed by way of birth certificate or other official identity documents.

8.6. The Issues Paper notes that access could be declined on the basis that it would be an unwarranted disclosure of the affairs of another individual.[37] However, there may be occasional particular cases where the disclosure might be warranted, for example where

[36] Issues Paper [12.63].
[37] Privacy Act 1993, s 29(1)(a).

the subject of the profile has died or where the DNA information is not available from other sources.[38]

8.7. I suggest that flexibility for familial access in these circumstances therefore needs to be accounted for. It may be appropriate to provide for court approval and oversight of any such application, noting the likely complexity of assessing the relative privacy interests in such cases.

9. Familial searching (chapter 13)

9.1. Familial searching is a lawful form of "forensic comparison" under the CIBS Act and is regulated by an unpublished Police protocol.[39] In my view, this technique should be reserved for use only as a last resort in serious cases and under robust oversight.

9.2. The Issues Paper notes the fundamental issues with the use of DNA profiles for familial searching, including the lack of consent by many who have provided samples to the known person databank (many of whom are not convicted offenders).

9.3. It would be appropriate, given the serious human rights and NZBORA issues arising, to create a warrant requirement so that the case for conducting a familial search can be made to an independent judicial officer for authorisation. The numbers of familial searches being conducted (101 in 15 years)[40] suggests that judicial oversight via a warrant process is not impractical as an option.

10. Retention of Samples and Profiles (chapter 14)

Samples

10.1. Law enforcement and criminal justice objectives tend to operate under a presumption that samples should be kept as long as possible (in case they are or become useful in future). By contrast, the privacy rights of individuals favour the setting of clear rules around retention and destruction. The purpose of collection and the nature of consent are relevant concepts here, as well practical considerations such as cost and efficiency.

10.2. The original purpose of collection (including any related purposes) needs to be considered in any reform of the rules around the retention of DNA samples. In 2009, the former Privacy Commissioner expressed concerns about the extension of the retention period for samples obtained from cleared suspects without adequate justification.

10.3. The collection of samples by consent is also relevant in developing policy around retention periods. A one-off consent to provide a sample, especially by a young person,

---

[38] One example is where the child of a rape victim seeks access to the genetic material of their parent for diagnostic purposes, where there is no other means of obtaining the DNA of the biological parent.
[39] Issues Paper at [13.39].
[40] Issues Paper at [13.10].

cannot be treated as a lifetime consent to the retention of their genetic material and information, and should be reviewed after a suitable period.

10.4. The Issues Paper notes efficiency as a competing factor and the cost of storage.[41] These are practical considerations that also inform when samples should be collected (in accordance with the statutory purpose) and how long they should be retained.

10.5. While I accept that in certain cases such as crime scene samples, it will be necessary to retain those samples for a considerable period, each purpose for which a DNA sample is obtained should inform and justify the appropriate retention period. The general principle is that samples may be retained until the primary use for that sample is spent, such as where law enforcement and evidential needs have passed and the offender no longer has an interest in that sample being retained.

10.6. In terms of the return of samples to individuals, this will be culturally important to some individuals but perhaps not to others. The importance of these issues to certain groups (including tikanga Māori) should inform the design of the rules around retention, return and destruction.

10.7. The Issues Paper reports that some work has been done by ESR to consider appropriate cultural approaches.[42] This work should be developed as necessary (including consultation with relevant stakeholders) to inform the appropriate approach to returning samples and to their destruction, and the extent to which individuals should be provided with choice and notification.

10.8. Once rules are developed, an audit approach would ensure compliance, and audit results could be reported to an appropriate oversight body. One option would be for the IPCA (or another oversight body) to receive audit results and consult with my Office and other relevant stakeholders on any particular trends or issues arising.

DNA profiles

(i) Security

10.9. The Issues Paper notes that while unauthorised access to the DNA databanks is an offence, the CIBS Act does not provide any particular oversight to ensure against inappropriate access, or to ensure the security of DNA profiles. One breach was reported in 2009.

10.10. Privacy breach notification is expected to become mandatory for sufficiently serious privacy breaches once the Privacy Bill is enacted.[43] The Law Commission could consider whether oversight of the DNA databanks would be suitably strengthened by including

[41] Issues Paper at [14.56].
[42] Issues Paper at [14.29].
[43] Privacy Bill 34-2, Part 6(1).

an express obligation to report any non-minor privacy breach affecting a databank to my Office.

10.11. The CIBS Act could require the Police and ESR to develop appropriate policies in relation to security, and to consult on those policies with my Office and appropriate stakeholders.

10.12. Privacy principle 5 requires an agency to ensure that personal information is protected by security safeguards that are reasonable in the circumstances, and that where the information is given to another person in connection with the provision of a service (such as the ESR providing a service to Police) that everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure.

(ii) Alignment with clean slate policies

10.13. In 2009, the former Privacy Commissioner submitted that there should be greater alignment between the retention periods for DNA profiles and the clean slate scheme. As the Issues Paper notes, the clean slate scheme is directed at the negative consequences of information being shared about a person's criminal past. This allows an individual to put their past behind them and to limit the stigmatising effects of their past acts.

10.14. The clean slate scheme does not erase all offending and has a number of relevant conditions (with exceptions for specified offences and custodial offences).

10.15. I support greater alignment by analogy with the clean slate scheme (as the Law Commission is considering)[44] as this supports the principle of limiting retention. This importantly helps an individual to live normally in society once the consequences of their past offending have been dealt with. This is consistent with the privacy principles that allow individuals to request the correction of personal information that is held about them (including the deletion of that information) to ensure it is up to date and not misleading, having regard to the purpose for which the information may lawfully be used.[45]

(iii) Crime Sample Databank

10.16. The Issues Paper sets out options for managing retention and removal of profiles from the CSD. As noted, one option would be for the Police and the ESR to develop a protocol or policy.[46]

10.17. A regular scheduled audit of the CSD against the protocol would ensure compliance, and audit results could be reported to an appropriate oversight body. Provision could also be made for unscheduled audits as instigated by an oversight body, or for

---

[44] Issues Paper at [14.114(b)].
[45] Privacy Act, s 6, IPP 7. See also the emerging privacy right to erasure discussed in the Privacy Commissioner's submission on the Privacy Bill Part A.7. https://www.privacy.org.nz/news-and-publications/reports-to-parliament-and-government/submission-on-the-privacy-bill/.
[46] Issues Paper at [14.120].

inspection. One option would be for the IPCA (or another oversight body) to receive audit results and consult with my Office and other relevant stakeholders on any particular trends or issues arising.

11. Oversight (chapter 15)

11.1. I support the proposal for greater oversight of the collection, analysis and use of DNA in criminal investigations. The challenge is to create an effective and efficient framework for oversight, commensurate with New Zealand's needs, size and machinery of government.

11.2. The emphasis in the Issues Paper is improving external oversight of the use of the DNA databanks. Options for strengthening internal governance arrangements are also worth exploring to achieve some of the policy objectives. External oversight will be more efficient and effective if the underlying governance arrangements are robust.

A one-stop shop or distributed oversight?

11.3. Overseas jurisdictions have established bodies to carry out oversight functions. It is clear that oversight can play a critical role in guiding the governance and operation of the databanks and ensuring compliance. The question for New Zealand is whether one oversight body should be created (or an existing body with added functions) to provide a "one-stop" shop, or whether the tasks can be shared across different oversight bodies to create a co-ordinated oversight framework (a "distributed" approach).

11.4. The distributed approach may be more efficient if different entities absorb particular tasks compared to one entity assuming the bulk of the oversight tasks. The distributed approach may bring a broader set of oversight skills and experience. However, this would require effective co-ordination and "joined-up" oversight between various entities so that issues do not fall between the cracks.

11.5. Consultation between oversight entities is a useful tool for linking oversight. For example, the Privacy Act allows my Office to consult with other oversight bodies on issues of mutual interest and overlaps between our respective jurisdictions.[47]

11.6. An Oversight Board (supported by a relevant Ministry such as the Ministry of Justice criminal justice team) could be considered.[48] This could be made up of the relevant entities that have an oversight role and other relevant stakeholders. It could be chaired by a lead oversight body, or the chair could periodically rotate. A Board model has the

---

[47] Privacy Act 1993, s 117 (Ombudsman), 117A (Health and Disability Commissioner), 117B (Inspector-General of Intelligence and Security).

[48] This is consistent with the 2009 recommendation of the former Privacy Commissioner set out at [15.76(b)]. A comparative model is the intelligence and security oversight group I convene made up of those entities having oversight responsibilities for the intelligence agencies including the Privacy Commissioner, the Inspector-General of Intelligence and Security, the Chief Ombudsman and the Auditor-General: https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioners-2015-annual-report-marks-a-year-of-big-changes/.

advantage of flexibility and can be adapted to accommodate a variety of members as it develops and if oversight needs change over time.

11.7. The Kaitiaki Group is another relevant model.[49] The National Kaitiaki Group considers applications for approval to disclose, use, or publish 'protected information', being information that is on or from the National Cervical Screening Programme Register and that identifies the woman or women to whom the information relates as being Māori.[50]

11.8. An Oversight Board or Group could meet annually or more regularly to report on the respective responsibilities and findings over the period, hear from the operational agencies (the Police and ESR) and stakeholders and make recommendations to Police for improved practice and any necessary legislative amendment to respond to issues arising. Those reports could be provided to the Ministers of Police and Justice and could be tabled in Parliament.

11.9. Table 1 in this chapter sets out the potential oversight tasks that the review has identified.[51] These are grouped as case-specific approvals, complaints, review, consultation/approval of policies, approval of technologies/techniques, auditing/monitoring compliance, reporting and public education/engagement.

11.10. As the Law Commission considers the development of an oversight framework, I am available to provide further comment on how these tasks could be allocated.

[49] The Kaitiaki Group established under the Health (Cervical Screening (Kaitiaki)) Regulations 1995
[50] The National Kaitiaki Group has certain criteria for assessing applications to access Māori women's data. These criteria ensure the use of data is consistent with the Kaitiaki Regulations. The applicant must show how they will use the information for the benefit of Māori women, address the principle of the sanctity of te whare tangata, and protect the information in a manner that is culturally appropriate.
[51] Issues Paper at pp 325-327.