

OFPC BACKGROUND INFORMATION FOR REVIEW OF PART 1D OF THE FORENSIC PROCEDURES PROVISIONS (CRIMES ACT 1914)

OFPC Documents

The Privacy Commissioner delivered this speech *Preserving Privacy in a Rapidly Changing Environment* to the Australian Institute of Criminology Conference in June 2001.

It sets out a framework* whereby new initiatives in law enforcement and crime prevention can be assessed for an appropriate and balanced privacy response. The full paper is available at www.privacy.gov.au/news/speeches/sp34note.doc

Extract (pp:12 - 14): CrimTrac and The National DNA Database

The Federal Government, in co-operation with State and Territory Governments, has established a national DNA criminal investigation system as part of the CrimTrac initiative. The DNA database system will contain DNA profiles of samples collected from suspects, offenders and volunteers by the police services of all Australian jurisdictions.

The value of DNA profiling as an item of evidence to link suspects or offenders to a crime scene is well recognised. Equally, DNA profiling can also rule out suspects or volunteers. Improvements in DNA testing technologies and the ability to produce 'digital' DNA profiles now make possible the use of IT and digital communications to accelerate the elimination and/or matching process. CrimTrac's National DNA Database is expected to have a significant impact on crime detection.

The move to establish an identification database based on DNA does carry privacy implications and risks. These depend amongst other things on how widely collection of identification material extends in the population, how the samples are collected, including whether with force, and how the DNA samples and information are used, disclosed and stored once collected.

As it has been established in Australia, the collection of DNA samples for law enforcement purposes has been targeted to criminal or suspected criminal activity and is subject to a range of checks and balances. Each of the States and the Commonwealth has introduced its own legislative and administrative approaches however they are all based largely on the Model Forensic Procedures Bill 2000 that was developed over a number of years by a representative working group. During the various stages of development there has been extensive public consultation, including with the Office. The consultation processes were supported with detailed discussion papers and were conducted openly with feedback provided at various stages. Privacy issues were raised and led to some adjustment of the settings – a reasonable balance was struck.

In terms of the decision-making framework outlined above, this process was conducted reasonably well. The implementation phase has not proceeded quite as smoothly. In legislating the model Bill in their own jurisdictions the States have decided on variations in approach that in some cases extend the collection of samples and lower the protections.

The impact of the variations on the overall scheme is still to be assessed. It is also the case that checks and balances in this system are continuing to evolve with experience and as issues emerge. The variations also appear to have had the unintended consequence of diminishing the utility of the CrimTrac database.

The overall operation and administration of CrimTrac has recently been considered by the federal Parliament in the context of the *Crimes Amendment (Forensic Procedures) Bill 2000* (the Forensic Procedures Bill) (the Bill was passed and is now the *Crimes Amendment (Forensic Procedures) Act 2000*).

The Senate Legal and Constitutional Legislation Committee (the Committee) recommended in its report on the Forensic Procedures Bill that the role of the Federal Privacy Commissioner be expanded to include oversight of the processes for the retention and destruction of DNA profiles, and the functioning of the DNA database within the laboratory. It also raised some issues about the overall supervision of the scheme that arise from its multi-jurisdictional nature.

This is an issue of *accountability* in terms of the framework set out above. The following discussion identifies the issues and the proposed solution. From a privacy perspective, a satisfactory accountability mechanism is an important step in implementing a system that has the potential for containing a large amount of highly sensitive personal information.

The Committee noted that the capacity of the Privacy Commissioner to oversee State and Territory forensic procedures regimes participating in CrimTrac is limited. It recommended that privacy issues be considered in inter-governmental agreements for CrimTrac, including cooperative oversight arrangements. One possible option is a system of co-ordinated oversight by the Ombudsmen, Privacy Commissioners and police supervisory authorities of participating jurisdictions. Fundamental to the effectiveness of this approach would be the ability for information about the forensic procedures regimes in participating jurisdictions to be exchanged between these authorities at least as freely as the information is able to be exchanged between participating law enforcement bodies.

The Privacy Commissioner's view is that effective oversight involves more than the CrimTrac agency and should involve auditing and monitoring on a periodic basis of:

- the separate Commonwealth, State and Territory forensic procedures regimes; and
- the operation of the national DNA database as a whole, particularly the interaction of the various forensic procedures regimes within the CrimTrac system.

The Minister for Justice & Customs, Senator Ellison responded to the issues raised in the report by making a commitment to pursuing the issue. He said in Parliament that

In addition to extending the legislation to include the Privacy Commission and the statutory review of Commonwealth forensic procedures, I have written to state and territory ministers with a view to getting agreement on cooperation between Commonwealth, state and territory bodies to ensure there is effective oversight of not only the operation of a DNA system within each jurisdiction but also the overall operation of the national system.

A more detailed extract from Senator Ellison's statement to Parliament is at Attachment 2.

ATTACHMENT 2

Extract from Minister for Justice & Customs, Senator Ellison statement of 5 March to Parliament about the accountability arrangements for CrimTrac (starts page 22342)

"In relation to the committee's fourth recommendation, I have engaged in discussions with the federal Privacy Commissioner and the Commonwealth Ombudsman in developing a response. Some serious issues have been raised in relation to the oversight of the national DNA database system. In addition to extending the legislation to include the Privacy Commission and the statutory review of Commonwealth forensic procedures, I have written to state and territory ministers with a view to getting agreement on cooperation between Commonwealth, state and territory bodies to ensure there is effective oversight of not only the operation of a DNA system within each jurisdiction but also the overall operation of the national system. This is best achieved by including formal independent monitoring mechanisms in the CrimTrac agreement with the states and territories so that the total scheme is properly audited and monitored. I am making these statements because I did undertake with the federal Privacy Commissioner that I would make these statements in reply in this debate. Of course, matters will no doubt be taken further during the committee stage.

"I might also mention that I expect to discuss oversight arrangements at the next meeting of the Australian Police Ministers Council in June. While recognising that CrimTrac is conscious of accountability issues and is constructive in the development of appropriate procedures, adequate and independent monitoring of a national DNA database system is critical if we are to have an effective system that ensures that any problems are quickly identified and remedied. The best way to do this is to ensure that there is adequate independent monitoring in each jurisdiction, and across the jurisdictions, which can, in turn, properly investigate complaints and pool information and better practices to safeguard information and ensure that DNA material is collected and matched in accordance with procedures. This is extremely important and must be addressed.

"The procedures in this legislation and the legislation of the states and territories are to be put in place to prevent an undue impact on the lives of individuals who provide DNA for the system and to ensure that information obtained from it is

used only for the purposes for which it is collected. It is therefore very important that we take steps to ensure that there is adequate independent oversight of compliance with agreed procedures. In view of the interjurisdictional nature of the scheme it is vital that we have arrangements that ensure that the oversight function is like the system itself: interconnected and properly coordinated. These arrangements must also ensure that complaints can be investigated easily without jurisdictional barriers becoming a problem. By encouraging compliance and avoiding problems later these measures will also play a role in improving the effectiveness and efficient use of the system by law enforcement agencies.

"I consider these issues can be addressed within the 12-month period before the proposed review, but in order to ensure that there is adequate follow-up on this issue it is proposed that the legislation be amended to provide for a further review within two years of that date if the review report indicates there are still deficiencies. This will cover the situation if there has been less progress than expected. So we have the review in 12 months and, if that reveals that there has not been the progress that was desired, then further review is possible within two years of that date. Let me make it clear: there is not just the one-off review; there is a facility for further review if matters have not progressed satisfactorily. Similar arrangements would also appear to be useful in relation to other elements of the CrimTrac system. I will also be taking up the broader application of the proposed monetary and accountability mechanisms with state and territory ministers.

"I now come to recommendation No. 4. The legislative changes proposed in relation to this recommendation are: firstly, to include the Privacy Commissioner on the independent review team; secondly, to ensure the independent review considers the effectiveness of the independent oversight and accountability mechanisms for the DNA database system; thirdly, to defer the review until 12 months after the commencement of these new provisions—this will enable the review to assess the procedures in light of an operational DNA database; and to assess progress in developing the accountability mechanisms. With this deferral we will be able to see how these provisions are operating in the meanwhile. There is a provision for a review due now but the government is of the view that this, perhaps, would not be worth while and wishes to defer it for 12 months and then have the review in the fashion mentioned.

"The final response is to cause the minister to ensure a further review is undertaken if the initial written report tabled identifies any inadequacies with the matters considered in the initial review—that is the review within two years after that first review that I mentioned. Proposed government amendment No. 27 deals with these matters. Proposed government amendment No. 24 merely adds the Commonwealth Ombudsman and joins the Privacy Commissioner as a person to whom database information can be disclosed without that disclosure constituting an offence. This amendment recognises the own motion investigation powers of the Ombudsman and will improve independent oversight of the legislation."

* This framework was further developed and included in the **OFPC Submission to the Senate Legal and Constitutional Legislation Committee Inquiry into Terrorism Bills – April 2002**

Extract (pp:2 - 5)

Section One – A Framework

Balance and Perspective: A Path to Effective Solutions

8. It is easy to argue that security necessarily comes at a cost to liberty. That is, we can only enjoy the right to feel safe and secure if we forgo certain other rights, such as the right to privacy. This is not necessarily the case. It is possible for people to have both privacy and security and they expect their parliament to provide them with both. For example, in the biometrics field, some airports are considering introducing body scanning technology that will help security staff identify hidden firearms and other devices. One version of this technology, being used in the USA, is a privacy invasive technique that scans a person and shows an image of each traveller's naked body in some detail on a computer screen. A privacy respecting version of the same technique is available that simply indicates to an officer the vicinity in which there may be a concealed weapon, without displaying the individual's naked body. The first technique is privacy invasive, while the second technique, which achieves the same outcome, is less so.¹

9. Admittedly, it is not always as simple as this in practice and there will be times when the only solution available to legislators involves a diminishment of our privacy and other rights. Such approaches, however, should always be the measure of last resort, used only after other options have been identified and rejected.

10. The challenge, then, is to find a fair and useful means of considering, weighing and making judgements about the seemingly competing priorities involved in a debate such as this. Identifying the parameters and community values is the key to determining how to address our need for security, while respecting privacy and having regard for other individual freedoms. This section outlines a framework that could prove useful in moving our community's deliberations forward in this area.

11. Arguably, the current challenges before our community and this Parliament are not new. Others before us have struggled with responses to threats of terrorism against their states and nations, with ranging degrees of success. Justice Kirby, in an address to

¹ Example used by Ann Cavoukian, Ph.D. Information and Privacy Commissioner of Ontario. Further reference available at: www.ipc.on.ca/english/pubpres/ext-pub/steps.htm

the 32nd Australian Legal Convention² in Canberra only a month after the events of 11 September 2001, offered an account of history in this regard. He reminded us of the terrorist challenges faced by Uruguay, Italy and Germany to name but a few.³ Justice Kirby, however, also offered salient guidance about the more successful approaches to such a challenge, including keeping our perspective, analysing the threat and responding in proportion to what we find.

12. Justice Kirby further cautioned that sometimes “it is wise to pause”, for “[the] countries that have done best against terrorism are those that have kept their cool, retained a sense of proportion, questioned and addressed the causes”.⁴ It is now more than six months since the events in the USA. Commendably, we in Australia have taken time to begin to think about how we might respond, about what those threats mean to our country and to our choices for how we live. The issues are complex and demand careful, balanced consideration – they are matters, which for all of us, are worth taking the time to get right.

13. Before considering the framework in more detail, there is a little more to say on perspective. Determining what our Australian perspective might be is a multi-faceted task. We need to try to consider the issue in both the shorter and the longer terms. For example, does the degree and type of threat we feel today differ from that which existed in the days and weeks after 11 September 2001; if so, how and why? Will the way we assess the issues today differ in the future? If we are uncertain, what does this say about the purported permanency of any measures put in legislation in the coming months? How do we weigh the risks and benefits of taking steps against a threat we may know today, but that may not be present in the future? If the measures remain, they may remain open to use for other purposes – what do we do to avoid ‘function creep’?

14. Often the best way to strike a good balance is to ensure there is ample public debate on the issues and that such debate is conducted in an open and transparent manner. Our search for perspective may be influenced also by our geographic location, our history and our cultural response to threats of the current kind. Is the nature of the threat and the proposed resultant change to things (such as the protection of our personal information) the same for us as for other nations; if not, why not? We should reflect on the proportionality of any proposed response, and in ways congruent with our perspective on world events.

15. The framework outlined here for considering new legislative responses that have a major impact on the community, by giving law enforcement agencies more intrusive powers, was first explored at the Australian Institute of Criminology’s conference in June 2001. Broader discussion can be found in the paper ‘Preserving Privacy in a Rapidly

² Kirby, J., ‘Australian Law – after September 11, 2001’, paper presented to the 32nd Australian Legal Convention in Canberra on 11 October 2001, which can be found at: www.highcourt.gov.au/speeches/kirbyj/kirbyj_after11sep01.htm

³ Op cit., pp. 4-5

⁴ Op. cit., pp. 6-7

Changing Environment'⁵ (this paper is attached to the submission). Critique of this framework has been sought in a number of forums, with a view to either improving it or replacing it with a better framework. So far though, the framework has attracted little criticism.

16. Further consideration and deliberation of security and privacy issues over recent months suggest the framework applies to matters not only about developments in domestic law enforcement, but also to those about broader safety and security in civilian society.

17. Essentially, the framework intends to bring about balance and perspective to considerations of legislative proposals with significant effects on privacy. It does so by leading us through seven key steps, including: defining the nature of the problem and the scope of possible responses to it; thinking about how new powers might be enacted; considering what the transparency, accountability and reporting requirements should be; and ensuring review of the mechanisms after a suitable period.

The Framework

Key step	Things to consider, including:
Identify the problem	<ul style="list-style-type: none"> ✓ Size & scope of the problem ✓ Likely longevity ✓ Implications in the Australian context
Identify the range of possible solutions	<ul style="list-style-type: none"> ✓ The range of responses open to us ✓ Resource implications of these options ✓ Efficacy issues – which option/s will work best and not unduly affect people's lives?
Think carefully and clearly about the proposed solution	<ul style="list-style-type: none"> ✓ What is the impact on privacy, and on whose privacy? ✓ Will the solution work and will it meet its target? ✓ What are the community's values here? ✓ Proportionality – is the measure proportional to the known risk?
What does the community think?	<ul style="list-style-type: none"> ✓ What consultation or debate has occurred? ✓ What does it tell us?
Implementing the new powers	<ul style="list-style-type: none"> ✓ Confer intrusive powers expressly in law (via an Act, not subordinate legislation) ✓ Legislation to state, expressly and objectively, the grounds on which the powers may be used ✓ Authority to exercise powers to rest at an appropriate level – to be expressly stated in legislation
Need to ensure transparency,	<ul style="list-style-type: none"> ✓ Make sure the community is kept informed about use of the powers

⁵ Office of the Federal Privacy Commissioner, 'Preserving Privacy in a Rapidly Changing Environment', paper presented at the Australian Institute of Criminology Conference called 'Future Directions, Crime Prevention, Legal Responses and Policy' on 22 June 2001 (COPY ATTACHED and available online at www.privacy.gov.au/news/speeches/sp34note.doc).

accountability and reporting	<ul style="list-style-type: none"> ✓ Ensure a transparent and independent complaints-handling system, monitoring system and the powers of independent audit ✓ Include an independent and public assessment and reporting process for the operation of the measures ✓ Ensure reporting and oversight powers are commensurate with the intrusiveness of the measures ✓ Preferably spell out these arrangements in legislation, especially where the new powers are particularly intrusive
Review processes	<ul style="list-style-type: none"> ✓ Parliamentary review of the measures after a fixed period – identify operational successes, as well as unintended or undesirable consequences ✓ Modify or remove powers as needed ✓ Include a ‘sunset clause’ – it is wise to pause and think again.

18. The latter two steps (outlined in the table above), reflect a vital process in ensuring that what we aim for in constructing anti-terrorism measures is just what we deliver. Not only this, but individuals have a reasonable right of complaint and should have available the option of redress by an independent body. The community expects to be told about how the use of these measures is progressing with regard to their effects upon the use of personal information.⁶ These steps, supplemented by the assurance that necessary monitoring and auditing maintains an effective and proportional overview of the measures, go far in maintaining community confidence that potentially intrusive actions are minimised, justified, exercised accountably and that they are reviewed.

19. Finally, building in a review of the measures helps guard against ‘function creep’ at a later date or the otherwise unnecessary retention of powers that risk losing their necessity as circumstances change. Two practical ways of achieving this outcome are to build into the legislation a trigger for parliamentary review, perhaps involving an assessment and report to that review by an independent body, or alternatively (and arguably more effectively) to insert a ‘sunset clause’ into the legislation. The latter step means that the law will lapse, so the parliament must look again at the circumstances and consider anew whether that which influenced the measures in the past, remains a consideration in the present. If so, further legislation would need to be passed.

20. It is in the context of seeking a truly proportional and appropriate response that this approach to considering the current anti-terrorism bills is presented. If “every erosion of liberty must be thoroughly justified”⁷, calm reflection will help to ensure the

⁶ OFPC Research ‘Privacy and the Community’ (Approx. 90% of those surveyed wanted to know what information about them was being collected and for what purposes it was being used.) The research is available at: www.privacy.gov.au/publications/rcommunity.html

⁷ Kirby, J., op. cit., p. 7

steps we are about to take are wise, effective, commensurate with the problems before us, open to appropriate scrutiny and likely to last for as long, or as short, a period as they are needed.

Biometrics and Privacy Paper

The Privacy Commissioner delivered this paper *Biometrics and Privacy – The End of the World as We Know It or the White Knight of Privacy* to the Biometrics Institute Conference in March 2002. The full paper is available at www.privacy.gov.au/news/speeches/sp80notes/doc

Extract (pp: 14 - 15):

Coverage of the Privacy Act

The Privacy Act covers Commonwealth public sector agencies and a fair part of the private sector. It is worth noting that this coverage leaves some gaps. For example, not all State or Territory public sectors are covered by State or Territory public sector legislation. Also, in the private sector, the Privacy Act does not cover most of the activities that employers carry out in relation to employee records. This could be of concern because biometric systems have a number of potential uses in the employment context, unless Federal and State workplace relations law provides sufficient protection.

The Government has announced that it will review in conjunction with the States existing Commonwealth, State and Territory laws to consider the extent of privacy protection for employee records and whether there is a need for further measures. The findings of this review are expected to feed into the general review of the Privacy Act mentioned earlier.⁸

Is biometric information personal information?

The Privacy Act applies to ‘personal information’. A threshold question is whether biometric information is personal information. The Privacy Act defines personal information to be:

‘Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.’ (Section 6)

⁸ The Government has established a review to answer this question; “Fact Sheet: Employee Records”, 22 December 2000, at www.law.gov.au/privacy/newfacts/EmployeeRecords.htm

Biometric information is clearly information about ‘an individual’. On the question of whether biometrics is identifying information the authors of “At face value” which include Dr Borking from the Registratiekamer in the Netherlands say that:

‘In the context of biometrical identification it can also be argued that this person is generally identifiable, since the biometrical data is used for identification or authentication, at least in the sense that the person concerned is distinguished from any other person.’

The authors go on to say that with this approach, the identifiability of the person does not depend on the availability of other data, which – jointly or separately – allow the person concerned to be identified.⁹

Of course the use of biometrics generally involves a number of transformative processes that involve manipulation of the data and may include mathematical transformation of the information into a code. The authors of “At face value” conclude that:

‘There is no reason to think that what applies to the human characteristic itself, would not apply to the digital representation of that characteristic, the templates which are composed on the basis of these representations, and to any subsequent transformation. As the process continues, the amount of detail will change, but the unique link with the person concerned is kept. It is reasonable therefore to conclude that the data involved will remain personal data in most, if not all stages of their processing.’¹⁰

Threats to bodily privacy

The Privacy Act regulates information privacy in the Commonwealth public sector and the private sector nationally. It does not directly address the issue of bodily privacy which is often addressed elsewhere in general law or statute law. However, both the Information Privacy Principles (IPPs) for the public sector and the National Privacy Principles (NPPs) for the private sector require that information be collected in a way that is not unreasonably intrusive. This may be adequate a protection in many cases but is unlikely to be an adequate in cases where a person has no choice about whether or not to give a biometric.

The issue of choice is likely to arise where governments are considering use of biometric. The first step in building in privacy here is to take account of at the decision-making phase. There will be some contexts for example, in law enforcement, where there will appear to be prima facie arguments for mandatory collection of biometric information. Even in these cases I strongly encourage a systematic consideration of issues such as any alternatives available, who the measure will affect, whether it is proportional to the problem and what safeguards might be needed. This approach is discussed in more detail

⁹ Dr R Hes; Mr Drs TFM Hooghiemstra; Drs JJ Borking; ‘At face value: on biometrical identification and privacy’ Registratiekamer, September 1999 p 17
www.registratiekamer.nl/cgi-bin/modules/print.cgi

¹⁰ See above p 17.

in a paper I presented last year to an Australian Institute of Criminology Conference in 2001.¹¹ One approach in cases where a government may require a person to provide a biometric in intrusive circumstances is to have a separate law governing the circumstances. For example, there are separate laws in some States where individuals are required under new laws to give DNA samples for law enforcement reasons there are separate laws.¹² In other cases, governments as well as private sector organisations are to be encouraged to build in choice and to think about necessary safeguards.

In the private sector, uses of biometrics that involve bodily intrusive collection methods are likely to be strongly resisted by consumers. However, consumer resistance is only possible where the market gives them real choice. The extent to which the market provides real choice to consumers in the privacy area is a matter on which I am currently keeping a close eye, in relation to a number of areas of operation of the new private sector provisions.

Genetics Inquiry Paper

The Privacy Commissioner is a member of the Advisory Committee to the Australian Law Reform Commission and Australian Health Ethics Committee Joint Inquiry into the protection of Human Genetic Information. This submission to the Inquiry was made in March 2002. The full paper is available at www.privacy.gov.au/publications/genesub.doc

Extract (pp: 41 - 46):

Balancing Interests in the right debate

46.1 Individual freedom and privacy are important facets of modern Australian life, as is protecting the community through effective law enforcement. An appropriate balance must be struck to ensure that the benefits of these differing public interests are maintained and promoted.

¹¹ Future Directions, Crime Prevention, Legal Responses & Policy
www.privacy.gov.au/news/speeches/sp34_files/frame.html

¹² For a description of some of these see Australian Law Reform Commission and Australian Health Ethics Committee Issues Paper *Protection of Human Genetic Information: Issues paper 26*, October 2001.p 370 at www.alrc.gov.au/publications/publis.html#Heading5

46.2 People want to be protected and to have their property protected. People also want their privacy, and their choices around their privacy, respected. This is not an easy challenge to meet, nor an easy balance to find, as outlined at the Australian Institute of Criminology (AIC) conference in 2001, in the paper *Preserving Privacy in a Rapidly Changing Environment* (OFPC, 2001c).

46.3 The intent in protecting privacy, and in this instance genetic privacy, is neither to unduly inhibit current law enforcement, nor to prevent law enforcement bodies from gaining benefit when new opportunities and technological developments arise. There is a clear need, however, to ensure an adequate level of assurance for Australian citizens that law enforcement functions operate as Parliament intended, and that they do not intrude upon individual privacy or other human interests any more than is absolutely necessary.

46.4 These issues are as significant in relation to forensic DNA testing as they are for other law enforcement initiatives. In the context of DNA testing, however, it is vital to draw attention to a distinction often missed, but fundamental to the debate. DNA testing can occur with two intentions in mind, either simply as means of identifying an individual with respect to a crime or crime scene, or to inquire after more detailed genetic data about that person. In the former instance, no more information is sought about the person than would be the case if taking a fingerprint; the latter case intends to uncover data about a person's genetic makeup. As it stands, it is the former, identification function that law enforcement agencies cite as the intention behind forensic DNA testing as currently practised.

46.5 The upshot of this distinction is significant for privacy. The discrete issues relating to identity-focused DNA testing revolve around a couple of special concerns, namely the collection of samples (for instance, from whom, by whom, when and how), and then the retention of those samples (for example, how securely, for how long and for what purposes). Beyond these matters, the issues arising from forensic DNA testing are little different from those linked to other law enforcement procedures. All require close consideration of the reliability of evidence, the security and integrity of data, the necessary checks and balances around authority to use and disclose the data, necessary transparency, and adequate independent mechanisms for complaint-handling, audit and investigation.

46.6 In this context, forensic DNA testing, when issues of collection and data retention are adequately resolved, is not *prima facie* a particularly special case. Things become more complicated, however, if the testing leads to the search for, or discovery of, other information about the person inferred from more detailed genetic analysis. At this point, however, the submission concentrates on the case of forensic testing solely as a means of law enforcement agencies identifying individuals. Yet, with regard to DNA testing of this type, the need to ensure appropriate privacy protection is well recognised. Police have expressed strong concern for the assurance of necessary safeguards surrounding the collection of their own DNA and have every right to do so (Wilkinson, 2002; Jackman,

2002). It goes without saying that the community needs to get these safeguards right for all concerned, be they police, suspect or convicted criminal.

Collection, Retention and Destruction of DNA Data – National Regulatory Consistency and the Model Forensic Procedures Bill

47.1 As noted above, the collection and retention/destruction of data appear to be the key matters for consideration in regard to privacy and identity-based DNA testing. The Issues Paper, for instance, raises concerns about the breadth of discretion available to law enforcement bodies when contemplating an approach to a suspect for consent to collect a forensic sample, or similarly when considering using powers to take a sample without consent. There are also jurisdictional variations with regard to the collection of DNA samples. Consequently, there may be such discretion for individual law enforcement officers so as to lead too often, to an inappropriate balance being struck between relevant public and private interests. This coupled with further differences between States, Territories and the Commonwealth in the rules governing collection of DNA samples can lead to a greater diminution of individuals' privacy.

47.2 Moreover, the relative vagueness or inconsistency in legislative obligations across jurisdictions regarding retention and destruction or de-identification of data (both data relating to a forensic sample and the sample itself) leaves much room for inconsistency in data handling, with significant potential for negative effects on privacy. With regard to data retention, in the context of forensic DNA testing for identification purposes, most significant are the rules for the retention and destruction of the DNA sample itself – as presumably the only data sought in relation to the sample is that needed for identity purposes. Destroying the sample at an appropriate time then prevents its further unwarranted use.

47.3 Both of these issues were addressed in the *Model Forensic Criminal Procedures Bill 1999* (the Model Bill), developed by the Standing Committee of Attorneys-General. This Bill was developed on the premise that it would be uniformly enacted by all States and Territories, as well as the Commonwealth Government. In a submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the subsequent *Crimes Amendment (Forensic Procedures) Bill 2000*, this Office stated that unless 'the Model Bill (was) adopted uniformly, the arrangements for the DNA system as a whole would allow an agency in one State to obtain information collected in another jurisdiction in circumstances that would not be allowed in its own State. This would be a diminution of the rights of the citizens of that State as established under that State's laws.' (OFPC, 2000d)

47.4 Yet, such uniform consistency has demonstrably failed to be enacted. In its absence different jurisdictions have developed, for instance, differing numbers and categories of indexes for forensic samples matching. There are now some 56 different indexes for forensic DNA samples across the Commonwealth, State and Territory jurisdictions, leading to over 3100 possible different types of index matching. Given the many

variations in the permitted types of matching that can occur, there are instances (as predicted) where one type of matching is lawful in one jurisdiction, but unlawful in another.

47.5 At least 33% of current index matches are not permitted under law, with a further 8% unresolved as to legal status and 6% permitted only in limited circumstances. As noted in the Issues Paper (at p. 391-92), the problems around national uniformity were identified by the Senate Legal and Constitutional Legislation Committee as ‘the most contentious aspect’ in the context of considering the proposed forensic procedures legislation.

47.6 Without moves to ensure national consistency, the risks to citizens’ rights, as foreshadowed over 18 months ago, become ever more apparent. It remains my view that the Model Bill, as originally intended in offering a national framework for DNA testing for law enforcement-related identity purposes, offers an adequate, minimum standard for the protection of such data in Australia. Consistent enactment of the Model Bill’s provisions across all participating jurisdictions would resolve matters of legislative inconsistency and vagueness, thereby lending assurance to the community that forensic DNA testing occurs with adequate reference to individuals’ privacy and other private interests.

National, Comprehensive and Independent Oversight

48.1 There is a need to ensure a proper, external oversight of the national DNA database. This is likely to be required whenever a powerful new law enforcement system is introduced. The potential of the new arrangements to collect and retain samples containing genetic information simply reinforces the need to ensure that the oversight arrangements are simple and effective. Indeed, continued public acceptance of the database surely rests on guarantees of accountability, and assurances that the database will be effectively and securely managed – with such management open to independent, third party scrutiny. Such oversight (involving regular monitoring, auditing and reporting by independent authorities) will provide an effective accountability measure, which in turn can prevent, detect or rectify systemic non-compliance with database regulations.

48.2 This approach is not new to law enforcement. Part VIII of the *Telecommunications (Interception) Act 1979* provides for the Commonwealth Ombudsman to inspect the records of federal police at least twice a year to ensure compliance with legislative requirements for the retention and destruction of interception records. The similarities in privacy intrusiveness between the investigative tools for telecommunications interception and the taking of forensic DNA samples, indicates that as independent oversight operates successfully for the former, it is surely similarly appropriate for the latter.

An approach to Consistent and Effective Complaint Handling, Audit and Investigation

49.1 There are risks in any multi-faceted system involving many agencies, regulators and jurisdictions for accountability processes to become piecemeal and ineffective, not providing the individual with a clear understanding of how complaints, audits and investigations are handled and by whom. It is inevitable, for instance, that a complaint will arise from a series of events that occur across more than one jurisdiction; this will quickly test the efficacy of the system.

49.2 In the context of a national DNA database, there is a need for all relevant agencies and their investigation bodies to cooperate to ensure effective complaint handling, and coordinated, effective audit and investigation processes. The system, overall, needs to rest upon adequate accountability and transparency.

49.3 These issues were clearly recognised by Senator Ellison (Federal Minister for Justice and Customs) in his speech to Parliament in March 2001, during the debate on the Commonwealth forensic procedures legislation. The Minister highlighted that ‘adequate and independent monitoring of a national DNA database system is critical if we are to have an effective system that ensures that any problems are quickly identified and remedied.’ (Ellison, 2001)

49.4 In the delivery of such accountability, the Minister made clear ‘it is vital that we have arrangements that ensure that the oversight function is like the system itself: interconnected and properly coordinated. These arrangements must also ensure that complaints can be investigated easily without jurisdictional barriers becoming a problem. By encouraging compliance and avoiding problems later these measures will also play a role in improving the effectiveness and efficient use of the system by law enforcement agencies.’(ibid.) A copy of the Minister’s speech is Attachment ‘A’ to this submission.

49.5 It is essential to achieve a cooperative approach on these issues. It remains possible, through collaboration between Commonwealth and State/Territory Ombudsmen, Police Authorities and the Privacy Commissioner, to settle on an approach to oversight that coordinates complaint handling, and ensures effective powers and processes for audits and ‘own motion investigations’. This can provide the necessary, free and confidential mechanism that will give the public confidence that complaints are investigated appropriately, that the database is adequately audited and that necessary investigation is undertaken.

49.6 The respective Ombudsmen, Privacy Commissioners and Attorneys-General/Ministers for Justice must continue to work together to get this national oversight system right. It is critical, however, that the work is seen through to resolution, and that such a system is delivered. Progress to date has been very slow and it needs to be accelerated. It was, therefore, pleasing and very important that in the passage of the Commonwealth forensic procedures Bill, provision was included to ensure that the operation of the national DNA database would remain under Parliamentary review not

only for the initial 12 months of operation, but for a further period of two years, in the event of the initial review finding inadequacies in its operation. However, we are well into the initial period and much work is still to be done to ensure adequate accountability for the national DNA database. There is a risk that even an extensive, two year period of monitoring may be insufficient at this rate of progress.

Future Uses for Forensic DNA Data

50.1 As technologies develop, so do the opportunities for more innovative and effective, and potentially intrusive, means of using genetic data in law enforcement, as in other areas. As discussed in the paper given at the 2001 AIC conference (OFPC, 2001c), before seizing the opportunities we must take stock and measure them against the risks, seeking to move forward with a balanced response.

50.2 There are two forms of development that may lead to ‘function creep’ in respect of existing law enforcement mechanisms or public policy in this area, and which can then present new challenges to privacy. Firstly, there are advances in comprehending what is already being done. What, currently, is regarded as ‘junk DNA’ (supposedly offering nothing beyond markers that can help to identify an individual), may be discovered to hold far more detailed information (Concar, 2001). If this occurs, what happens to this potential data will need to be reviewed, since it is collected (though previously unwittingly) through a law enforcement process. Alternatively, consideration may need to be given to what happens to the process itself to ensure such data is not gathered. Consideration should be given to the responses to new tests, which, from the outset, will purport to be genetic tests intended to form a part of the law enforcement armoury.

50.3 In considering new developments, there are a number of questions to be asked and assurances sought. Will the technological solution achieve what is wanted, and in relation to the people for whom it is intended? Does the solution involve unintended discrimination? The efficacy of the proposed solution should be assessed and others’ experiences with similar developments sought; or if it is a wholly new initiative, careful testing must be conducted. We as a community should engage in public debate. We must seek to ensure proportionality: that is, balancing the degree of intrusion of the new tool with the nature and impact of the activity that is being prevented or investigated.

50.4 If the decision is to proceed to adopt and use the new technology, there are still things to do to maintain parity between law enforcement and individual freedoms. Any new intrusive powers for law enforcement bodies should be conferred expressly through law; which also expressly and objectively states the grounds upon which the intrusive power may be exercised.

50.5 Also necessary are clear measures of transparency and accountability, involving reporting to the community on the use of the powers, transparent and independent complaints-handling systems and independent monitoring, auditing and investigation in

relation to the operation of the powers to determine their need for modification or removal.

50.6 Significant changes to, and especially the weakening of, the regulation of law enforcement initiatives, such as the national DNA database, must be carefully contemplated. As with the uptake in technological developments, the impact upon privacy protection must be considered. People are well to be wary of ‘function creep’ through incremental change to the rules; such as a move from collecting DNA for the purpose of identity to collecting it because it offers (or may do so at some later date) greater genetic insight into those involved in criminal investigations and activities. Instead, we should consider significant changes to the use of genetic and other personal information consciously, openly and transparently.

50.7 Institutions have a responsibility to identify changes to policy intent, and to review the balance point between society’s interests in law enforcement and our interests in privacy and other freedoms. Such changes in policy should involve changes to legislation and regulation. Before starting down this path, the debate about change must be public. These are issues of such moment that they require public debate led by policy-makers and law-makers alike. The community needs to know what it stands to lose and what it stands to gain. Only then can we, as individuals and as a society, make a free and informed choice about how we are to proceed.

Inquiry into the *Crimes Amendment (Forensic Procedures) Bill 2000*.

In November 2000 the Privacy Commissioner made a *Submission to the Senate Legal and Constitutional Legislation Committee Inquiry into the Crimes Amendment (Forensic Procedures) Bill 2000*. The full Submission is available at www.privacy.gov.au/publications/cab.doc

INTERNATIONAL DEVELOPMENTS

Canadian Biotechnology Advisory Committee, *Genetics, Privacy and Discrimination*, http://www.cbac-cccb.ca/documents/en/GenPriv_Discrim_Oscapella.pdf

- A paper providing a general discussion of genetics and privacy issues, including international initiatives and developments. Issues include the tensions between the potential benefits and harms of genetic technology, and whether individuals have a residual right to genetic privacy.

Solicitor General of Canada, *Establishing A National DNA Data Bank: Summary of Consultations*, <http://www.sgc.gc.ca/epub/pol/e199611/e199611.htm>

- On 18 January 1996, the Solicitor General of Canada released the consultation paper *Establishing a National DNA Data Bank*, as part of Phase II of the federal government's DNA initiative. The consultation paper explored several key issues, including: who should be required to have their DNA data banked; when should biological samples be collected from convicted offenders and who should collect them; whether or not biological samples, in addition to the data, should be retained; and how DNA casework and data banking should be funded. It also provided background information on how the use of DNA can assist the police and the courts.

Office of the Privacy Commissioner of Canada, *Genetic Testing and Privacy*, http://www.privcom.gc.ca/information/02_05_11_e.pdf

- The Canadian Privacy Commissioner's report on genetic testing and privacy includes discussion on technical and scientific aspects, including genetic testing for forensic purposes, as well as a comprehensive analysis of privacy and civil liberties issues.

Information and Privacy Commissioner/Ontario, *Submission to the Ontario Law Reform Commission Project on Genetic Testing* <http://www.ipc.on.ca/english/pubpres/reports/gentest.htm>

- A brief submission discussing, in broad terms, civil liberty and privacy issues associated with DNA testing and databases, including in law enforcement and criminal justice matters.

**UK Human Genetics Commission, *Human Genetic databases*,
<http://www.hgc.gov.uk/topics.htm#ddna>**

- Links from the Human Genetics Commission website to documents dealing with Human Genetics databases (including forensics and criminal databases).

**UK House of Lords, Select Committee on Science and Technology – Fourth Report, *Human Genetic Databases: Challenges and Opportunities*,
<http://www.parliament.the-stationery-office.co.uk/pa/ld200001/ldselect/ldsctech/57/5701.htm>**

- A substantial nine chapter report of the Committee's investigation into human genetic databases. Although focused on medical applications of DNA databases, there is some discussion of specific applications of genetic technology in the field of forensic science (in particular, see Chapter 4).