IN THE MATTER OF THE ROYAL COMMISSION INTO FAMILY VIOLENCE

REVISED STATEMENT OF DAVID GEOFFREY WATTS

Date of document: 11 August 2015 Filed on behalf of: State of Victoria Prepared by: Victorian Government Solicitor's Office Level 33 80 Collins Street Melbourne VIC 3000	[redacted]

I, **DAVID GEOFFREY WATTS,** Commissioner for Privacy and Data Protection, SAY AS FOLLOWS:

INTRODUCTION

1. In September 2014, I was appointed as the inaugural Commissioner for Privacy and Data Protection (**Commissioner**).

2. My background is as a lawyer who has practised in both the private and public sectors, specialising in information technology, information privacy, intellectual property, governance and regulatory systems.

3. Before being appointed Commissioner, I was the Commissioner for Law Enforcement Data Security from November 2008 to September 2014 and the Acting Victorian Privacy Commissioner from April 2013 to September 2014.

4. From September 2005 to November 2008, I was the Assistant Secretary, Legal Services Branch, of the Commonwealth Department of Health and Ageing in Canberra. In this role I led the National Health Information Regulatory Framework project to support the development of Australia's national e-health system. I designed its regulatory scheme. The scheme is probably the largest and most complex Australian information sharing initiative. I also designed other information sharing-based initiatives, including the national registration and accreditation scheme for registered health professions and information sharing arrangements designed to curtail prescription shopping.

5. Previously, I headed the legal branch of the former Department of Human Services in Victoria from September 2002 to September 2005, where I was involved in the development of social policy-based legislative initiatives including the *Children, Youth and Families Act 2005* (**CYF Act**).

6. In October 2014, I was appointed to the Data Protection Advisory Group of the United Nations Global Pulse project. UN Global Pulse is an initiative of the UN Secretary General. It seeks to harness the benefits of big data whilst simultaneously respecting privacy. It is based on a recognition that digital data provides an opportunity to gain a better understanding of changes in human well-being and to obtain real-time feedback on how well policy responses are working. I am the only Australian representative.

SCOPE OF STATEMENT

7. I make this statement in response to a notice given to me by the Royal Commission into Family Violence pursuant to section 17(1)(d) of the *Inquiries Act 2014* to attend to give evidence and to provide a written statement prior to attending in relation to the matters outlined in Module 20 - Information Sharing.

8. This statement is made in addition to my submission made to the Royal Commission in response to the Commission's Family Violence Issues Paper, released on 31 March 2015. A copy of the submission is **Attachment DW-1**.

OVERVIEW OF PRIVACY

Privacy

9. 'Privacy' is an overburdened concept. One of the foremost international experts on privacy, Daniel Solove, has observed that there are a "welter of different conceptions of privacy" and has developed a taxonomy of privacy. In an article in the *California Law Review* ("Conceptualising Privacy" (2002) 90 Cal L Rev 1087), he argues that privacy consists of six main concepts:

   9.1 the right to be let alone;

   9.2 limited access to the self – the ability to shield oneself from unwanted access by others;

   9.3 secrecy – concealment of certain matters from others;

9.4 control over personal information – the ability to exercise control over information about oneself;

9.5 personhood – the protection of one's personality, individuality and dignity; and

9.6 intimacy – control over, or limited access to, one's intimate relations or aspects of life.

10. Privacy is not an absolute right. It is widely recognised that there can be departures from privacy where there is a countervailing public interest.

11. Based on a 1930s decision of the High Court in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, for many years it was accepted that there is no common law right to privacy in Australia. However, this interpretation was thrown into doubt by the more recent decision in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, in which the High Court decided that *Victoria Park Racing* was a decision about property law, not privacy, and did not stand in the path of the development of a cause of action for breach of privacy.

12. Although the question of whether the law recognises a common law right to privacy remains open, there is specific High Court authority about the more limited, fourth aspect of Solove's taxonomy of privacy, referred to in paragraph 9.4 above – control over personal information.

13. In *Johns v Australian Securities Commission* (1993) 178 CLR 408), the High Court decided that when a statutory power is provided to require the provision of information for a particular purpose, the extent of the dissemination of that information is limited by the purpose for which the power was conferred. Brennan J (with whom Dawson, Gaudron and McHugh JJ agreed) stated (at 423):

> Information is intangible. Once obtained, it can be disseminated or used without being impaired, though dissemination or use may reduce its value or the desire of those who do not have it to obtain it. Once disseminated, it can be disseminated more widely. A person to whom information is disclosed in response to an exercise of statutory power is thus in a position to disseminate or to use it in ways which are alien to the purpose for which the power was conferred. But when a power to require disclosure of information is conferred for a particular purpose, the extent of dissemination or use of the information disclosed must itself be limited by the purpose for which the power was conferred. In other words, the purpose for which a power to require disclosure of information is conferred limits the purpose for which the information disclosed can lawfully be disseminated or used.

14. Although *Johns* does not seem to be a widely known decision, Brennan J's analysis was subsequently approved by the High Court in *Katsuno v The Queen* (1999) 199 CLR 40. On its face, *Johns* applies to all information, not just personal information, and represents the position at common law. As I will explain below, Victoria's information privacy law permits significantly broader information sharing than the common law.

15. Australia is one of the few countries within the common law tradition where there is no common law right to privacy. In the USA, the Restatement (Second) of Torts recognises four privacy torts. In New Zealand, the decision in *Hosking v Runting* [2003] 3 NZLR 385 recognised a common law tort of serious invasion of privacy.

16. In Canada, privacy interests are protected from government intrusion by the protection against unreasonable search and seizure in section 8 of the Canadian Charter of Rights and Freedoms. Some provinces recognise a right of privacy at common law.

17. The United Kingdom is required to comply with the *European Convention on Human Rights* (**ECHR**). Article 8 of the ECHR confers a right to privacy that is consistent with Article 17 of the *International Covenant on Civil and Political Rights* (**ICCPR**). The way in which this international law privacy obligation has been implemented by the United Kingdom courts has been to absorb the Article 8 rights into what is known as the action for extended breach of confidence. In *OBG Limited v Allan* [2008] 1 AC 1 at 72 [255], Lord Nichols stated:

> As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct. In some cases information may qualify for protection both on grounds of privacy and confidentiality. In other instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy.

18. Despite the fact that the Australian Law Reform Commission has recommended the enactment of a privacy tort on a number of occasions, as has the Victorian Law Reform Commission and the New South Wales Law Reform Commission, these recommendations have not been implemented. In Victoria, there have been suggestions in some decisions (for example, in *Giller v Procopets* (2009) 24 VR 1) that the approach adopted in the United Kingdom – the extended action for breach

of confidence – might be adopted. Recent Western Australian authority (*Wilson v Ferguson* [2015] WASC 15) is to the same effect.

19. That said, it remains the case that there is no general right to privacy at common law in Victoria. Section 13 of the *Charter of Human Rights and Responsibilities Act 2006* (**Charter**) embodies a right to privacy that is consistent with Australia's international law obligations under Article 12 of the Universal Declaration of Human Rights and under Article 17 of the ICCPR. Although the Charter does not confer actionable rights on individuals, public sector organisations must act consistently with it. It follows that public sector-initiated responses to family violence must be informed by their Charter obligations.

Victoria's information privacy law

20. Victoria's legislative approach to privacy has centred on the fourth category of Solove's privacy taxonomy – control of information about oneself (see paragraph 9.4 above). This is commonly referred to as 'information privacy'.

21. There are two pieces of Victorian legislation that govern information privacy.

22. The first is the *Privacy and Data Protection Act 2014* (**PDPA**), which replaced the *Information Privacy Act 2000* and the *Commissioner for Law Enforcement Data Security Act 2005* with effect from 17 September 2014. The PDPA governs the collection and handling of personal information (but not health information) in the Victorian public sector and, uniquely, provides for the establishment of a protective data security regime for the Victorian public sector. The security regime will not apply to certain health services.

23. The second piece of legislation is the *Health Records Act 2001*, which governs the collection and handling of health information in both the public and private sectors in Victoria. It is regulated by the Office of the Health Services Commissioner.

24. For the purposes of this statement, I have not included an analysis of the *Privacy Act 1988* (Cth). It is also information privacy legislation. It applies to the Commonwealth public sector and a small part of the private sector.

The PDPA

25. The information privacy provisions of the PDPA are based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (**OECD**

Guidelines), which were developed by an expert group chaired by the Honourable Michael Kirby AC CMG and first published in 1980. They were subsequently the subject of extensive review by the OECD. The review affirmed the continued relevance of the OECD Guidelines and, in 2013, some minor changes were made. The current OECD Guidelines are embodied in the OECD Privacy Framework (**Attachment DW-2**).

26. The OECD Guidelines form the basis of all international information privacy law. Although there are jurisdiction-to-jurisdiction variations in the way they are implemented, they are the universal information privacy law benchmark. The *Information Privacy Principles* (**IPPs**) that comprise Schedule 1 to the PDPA are based on the OECD Guidelines.

27. The OECD Guidelines were developed by an organisation whose predominant concerns focus on economic issues, not human rights. The OECD's stated mission is 'to promote policies that will improve the economic and social well-being of people around the world'.

28. The OECD Guidelines were developed in a pre-internet, mainframe computing era, in response to concerns that cross-border information flows, particularly in the banking and insurance sectors were being impeded. This is because States were reluctant to permit their citizens' personal information to be sent across territorial borders unless the receiving State protected the information in the same manner as the sending State. The OECD Guidelines addressed this problem by proposing an information privacy framework that both protected information privacy whilst *simultaneously* promoting the free flow of information. This principle is embodied in the objects stated in section 5 of the PDPA, which include:

> (a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector

29. In my view the OECD's approach remains the appropriate model for Victoria's information privacy law.

30. The PDPA is *default* legislation. Its information privacy provisions apply to the public sector except to the extent that they are inconsistent with other legislation (see section 6).

31. In respect of the collection and handling of personal information, the PDPA retained key elements of the *Information Privacy Act*, most notably the scope of the public sector organisations to which the information privacy provisions of the PDPA apply (section 13) and the IPPs set out in Schedule 1.

32. The principal information privacy obligation in the PDPA is that an organisation (defined in section 3 to mean the public sector organisations in section 13) must not do an act, or engage in a practice, that contravenes an IPP in respect of personal information collected, held, managed, used, disclosed or transferred by it (section 20(1)).

33. This prohibition does not apply if the act or practice is permitted under one of the following of the PDPA's flexibility mechanisms:

    33.1 a public interest determination;

    33.2 a temporary public interest determination; and

    33.3 an approved information usage arrangement.

34. These new flexibility mechanisms were not in the *Information Privacy Act*. The evident intention behind the inclusion of these new mechanisms in the new legislation was to ensure that an authorising process was readily available to ensure that information privacy did not impede the free flow of information – information sharing – where there is a substantial public interest in so doing. They were expected to significantly assist in the delivery of public services in the public interest, in particular in areas such as child protection programs where multiple agencies hold information (see Second Reading Speech for the Privacy and Data Protection Bill 2014 (**Attachment DW-3**).

35. I describe each of these exceptions below under the heading "Flexibility mechanisms under the PDPA".

The Health Records Act

36. Health information privacy is regulated by the *Health Records Act*, which is administered by the Victorian Health Services Commissioner appointed under the *Health Services (Conciliation and Review) Act 1987*. The Health Privacy Principles, which are similar to IPPs, comprise Schedule 1 of the *Health Records Act*.

Other Victorian legislation

37. Other Victorian legislation also has an impact on information privacy, such as the:

37.1 *Freedom of Information Act 1982*, in respect of access to documents containing personal information; and

37.2 *Public Records Act 1973*, in respect of retention and destruction of documents containing personal information.

38. In addition, individual pieces of legislation contain provisions that limit, restrict or prohibit the use or disclosure of information, including personal information. By virtue of section 6(1) of the PDPA, these provisions operate to the exclusion of the PDPA. Typically these provisions take the form of confidentiality or secrecy provisions.

39. Confidentiality is a different concept from privacy, although they are related. In circumstances of confidence, the recipient of information generally owes an obligation of confidence to the provider, unlike privacy, which is the right of the subject of the information, no matter who provided or received it. An example of a statutory confidentiality obligation is that contained in section 464ZGK of the *Crimes Act 1958*, which concerns disclosure of DNA information.

40. Secrecy comprises techniques to prevent information becoming known by others. It may assist individuals to maintain confidentiality, companies to maintain confidentiality, and governments to serve other public interests, such as protection of national security. An example of a secrecy provision is section 33 of the *Emergency Services Telecommunications Authority Act 2004*.

41. Other legislative provisions potentially relevant to information sharing in the family violence context include:

41.1 provisions of the CYF Act that specify what the Secretary must or must not disclose in relation to foster carers and out of home carers;

41.2 Part 9E of the *Corrections Act 1986*, which contains extensive provisions regulating disclosure of information about prisoners and other individuals; and

41.3 Part 4 of the *Sex Offenders Registration Act 2004*, which regulates, among other matters, access to and disclosure of personal information from the

Sex Offender Register, for which the Chief Commissioner of Police is responsible.

Data security

42. IPP 4 (Data Security) has always required the Victorian public sector to handle personal information securely. It requires public sector organisations to protect the personal information they hold from misuse and loss from unauthorised access, modification or disclosure. However, Parts 4 and 5 of the PDPA set out new provisions relating to, respectively, the security of public sector data including personal information and law enforcement data. While Part 4 is intended, with limited exceptions, to apply across the whole of the Victorian government, Part 5 applies only to Victoria Police and the Chief Statistician, together with his or her employees or consultants.

43. Data security standards are intended to support and enable public sector organisations to undertake their functions efficiently, by ensuring that the right people have the right information at the right time. Frequently, data security is mistakenly seen in one-dimensional terms as exclusively concerned with confidentiality – in other words, keeping information in. Properly conceptualised, security supports information integrity and appropriate information sharing as well. The three pillars of a data security regime are:

    43.1 confidentiality – limiting official information to authorised persons for approved purposes;

    43.2 integrity – ensuring that information has been created, amended or deleted only by the intended and authorised means and is correct and valid; and

    43.3 availability – ensuring ready access to information by authorised persons.

44. Data security is of critical importance in the family violence context. Unauthorised access or disclosure of information can compromise the safety of individuals at risk of family violence. Conversely, failure to ensure that the right people have access to the right information at the right time can be equally harmful. As I said in the 2013-2014 Annual Report of the Commissioner for Law Enforcement Data Security (**Attachment DW-4**, at page 4), the tragic case of the murder of Luke Batty in February 2014 serves to highlight the consequences of approaching security too narrowly and of privileging confidentiality (ie, protecting information from

unauthorised disclosure) over the equally important elements of integrity and availability.

Protective data security

45. Under Part 4 of the PDPA, the Commissioner is obliged to develop the Victorian protective data security framework and may issue standards for the security, confidentiality and integrity of public sector data and access to public sector data. "Public sector data" is defined in section 3 of the PDPA to mean any information (including personal information) obtained, received or held by a public sector agency or other body to which Part 4 of the Act applies, whether or not the agency or body obtained, received or holds the information in connections with the functions of that agency or body.

46. Based on a range of existing international, Australian and State standards and guidelines, I have developed draft protective data security standards, which are intended to support Victorian government service delivery functions and reflect contemporary data security standards. A copy of the final draft of the protective data security standards, published within the Victorian public sector for comment in July 2015, is provided at **Attachment DW-5 (Draft Victorian Protective Data Security Standards)**. These standards have been the subject of extensive consultation and are expected to be publicly released in about December 2015.

47. The Draft Victorian Protective Data Security Standards consist of 20 high-level standards (which establish *what* has to be done), a corresponding objective for each standard (which sets out *why* it has to be done), protocols for each standard (describing *how* it should be done) and elements for each standard (which provide non-mandatory guidance about how to implement the standards and protocols). They address such matters as governance, policies and systems, security approval of all participants, risk management plans, information and communications technology (**ICT**) requirements and physical security. Standard 15 relates to information sharing and requires public sector organisations to develop secure information sharing practices to prevent the unauthorised sharing of public sector data.

48. The draft Victorian Protective Data Security Standards also emphasise the need for executive investment in and sponsorship of the data security measures required by the standards. I will refer to the need for high level engagement with privacy and security issues below in the context of barriers to information sharing.

49. There is substantial, but not complete, overlap between those agencies to which the privacy and data security provisions of the PDPA apply. For those agencies to which Part 4 applies, public sector body Heads are responsible for compliance with protective data security standards in respect of the data their body collects, holds, manages, uses, discloses or transfers, including for their contracted service providers, and for relevant data systems (section 88).

50. Part 4 also provides that, within two years of the issue of relevant protective data security standards, public sector body Heads must ensure that a security risk profile assessment is undertaken for their agency or body, and a protective data security plan is developed that addresses the relevant standards.

Law enforcement data security

51. Part 5 of the PDPA permits the Commissioner to issue standards for law enforcement data security (**SLEDS**). The latest such standards were issued in September 2014. A copy of the SLEDS is provided at **Attachment DW-6**. Victoria Police must not do an act or engage in a practice that contravenes a law enforcement data security standard, in respect of: (a) law enforcement data collected, held, used, managed, disclosed or transferred by it; or (b) law enforcement data systems kept by it (section 94 of the PDPA).

52. Chapter 4 of the SLEDS applies to the release, or disclosure, of law enforcement data. Standard 11 provides that release of law enforcement data must only occur if that disclosure is authorised and Victoria Police must ensure that agreements with approved third parties include the requirement that release of law enforcement data must only occur if it is authorised. Underneath this standard, there are several protocols which represent the minimum mandatory requirements to be addressed, in order to meet each standard. Protocol 11.1 provides that users must not release any information except where the release or communication of that information is authorised by law and/or Victoria Police policy.

PROHIBITION ON DISCLOSURE AND PERMITTED DISCLOSURES UNDER THE PDPA

53. IPP 2 governs the use and disclosure of personal information collected by relevant organisations. IPP 2.1 provides that an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless one or more of a number of specified circumstances exist.

54. Permitted disclosures may be made under the PDPA in three circumstances:

54.1 pursuant to the exemption in section 15 for law enforcement agencies;

54.2 pursuant to an exception in IPP 2.1; and

54.3 pursuant to one of the "flexibility mechanisms" in Part 3.

Publicly available information

55. First, however, it is important to recognise that there is no prohibition on disclosure of publicly available information, as defined in section 12 of the PDPA, because that Act does not apply to it. In relation to information sharing, the most significant category of publicly available information is that set out in a generally available publication, such as a telephone directory, newspaper or published reasons of a court or tribunal.

Exemption for law enforcement agencies

56. The exemption in s 15 in Part 3 applies to law enforcement agencies. These include not only Victorian, State, Territory and Federal Police, but also entities including the Youth Parole Board and agencies responsible for performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction for a breach. The exemption relevantly permits non-compliance with IPP 2.1 (among other IPPs) if the law enforcement agency believes on reasonable grounds that non-compliance is necessary:

56.1 for the purposes of one or more of its, or any other law enforcement agency's law enforcement functions or activities; or

56.2 in connection with the conduct of proceedings commenced, or about to be commenced, in any court or tribunal.

57. In the case of Victoria Police, the exemption also applies for the purposes of its 'community policing functions'. These functions are not defined in the PDPA, but the term is intended to refer to such roles as locating missing persons, providing necessary responses in public emergency and disaster situations, and locating next of kin if required (see the Explanatory Memorandum to the Privacy and Data Protection Bill 2014, clause 15 (**Attachment DW-7**)).

Exceptions under IPP 2.1

58. IPP 2.1 contains exceptions to the general principle that an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection. The primary purpose flows from the organisation's overall, legislated purposes and functions.

59. I consider a number of the IPP 2.1 exceptions to be especially relevant to information sharing in the family violence context. These are:

59.1 IPP 2.1(d)(i), which authorises disclosure of personal information where an organisation reasonably believes that use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare;

59.2 IPP 2.1(e), which authorises disclosure of personal information where an organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; and

59.3 IPP 2.1(g)(i) and (v), which authorises disclosure of personal information where an organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the circumstances described by or on behalf of a law enforcement agency. These circumstances include the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction.

60. The research exemption at IPP 2.1(c) is also very important. Once information about individuals is properly de-identified so that it no longer constitutes 'personal information', aggregated data can yield important insights into the incidence of family violence correlated against criteria such as type, location, age of victim and offender and the like.

61. Finally, the exception at IPP 2.1(b) provides that if an individual has consented to disclosure, an apparently attractive permission to disclose is offered. However, in my experience, it can be difficult in practice for organisations to obtain the valid consent required, especially where vulnerable or large numbers of individuals are concerned.

62. In November 2011, the former Office of the Victorian Privacy Commissioner published guidance as to the interpretation of the IPPs: *Guidelines to the Information Privacy Principles*, which largely remains current. A copy of the Guidelines is provided at **Attachment DW-8**.

Flexibility mechanisms under the PDPA

63. As I have referred to above, Part 3 of the PDPA establishes three mechanisms with the potential to facilitate information sharing:

63.1 public interest determinations (**PIDs**) and temporary public interest determinations (**TPIDs**);

63.2 information usage arrangements (**IUAs**); and

63.3 certification.

64. The first two of these mechanisms operate by reason of the provision in s 20 of the PDPA, whereby the requirement for organisations to comply with IPPs does not apply if the act or practice is permitted under a public interest determination, a temporary public interest determination or an approved information usage arrangement.

65. In October 2014, I issued guidelines in respect of all aspects of the above flexibility mechanisms, including interpretation of key terms and guidance as to how to make an application. A copy of the *Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arrangements and Certification* (October 2014) is provided at **Attachment DW-9**. Diagram 1 in the Guidelines (at page 8) assists organisations to decide which of these mechanisms may suit their needs. In particular, the diagram indicates that where there are multiple parties and/or complex arrangements envisaged, an IUA rather than a PID or TPID is the most suitable mechanism.

Public interest determinations and temporary public interest determinations

66. PIDs and TPIDs are loosely based on the mechanisms of the same name found in Part VI of the *Privacy Act 1988* (Cth).

Public interest determinations

67. A PID made by the Commissioner is a written determination under Part 3 Division 5 of the PDPA that, where a specified act or practice of an organisation might otherwise breach an IPP (other than IPP 4 - Data Security or IPP 6 - Access and Correction) or approved code of practice, it will not be regarded as having done so while the PID is in force.

68. Section 31(1) of the PDPA provides that the Commissioner may make a PID on application under section 29 if satisfied that the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with the specified IPP or approved code of practice. Any such determinations are to be published on the Commissioner's website.

69. Section 42 of the PDPA provides that both PIDs and TPIDs may be disallowed by either House of Parliament, consistent with Parliament's appropriate oversight of my power as Commissioner to make determinations that modify the operation of Victorian legislation.

70. To date, my Office has not received any application for a PID.

Temporary public interest determinations

71. The key differences between PIDs and TPIDs are that:

    71.1 whereas PIDs are in force until any expiry date specified, revocation or disallowance, TPIDs can last no longer than 12 months; and

    71.2 TPIDs have a shorter application process, reflecting their intended use in more urgent situations.

72. To date, my Office has consulted with a number of organisations when they were in the early stages of considering whether to make an application for a TPID. Where proposed disclosure was in issue, it was my view that most of these organisations could lawfully disclose the subject personal information under provisions of the PDPA without the need for a PID or TPID.

Information usage arrangements

73. The IUA mechanism in the PDPA is loosely based on a similar mechanism considered by the New Zealand Law Commission prior to its recommendation that

an information sharing mechanism be inserted into New Zealand privacy legislation. A copy of the New Zealand Law Commission's Ministerial Briefing on Information Sharing, 29 March 2011, is provided at **Attachment DW-10**.

74. An IUA is defined in section 45 of the PDPA as an arrangement that:

74.1 sets out acts or practices for handling personal information to be undertaken in relation to one or more public purposes; and

74.2 for any of those acts or practices, does any one or more of the following:

(a) modifies the application of a specified IPP (other than IPP 4 or IPP 6) or an approved code of practice;

(b) provides that the practice does not need to comply with a specified IPP (other than IPP 4 or IPP 6) or an approved code of practice; and/or

(c) permits handling of personal information for the purposes of an 'information handling provision', as defined in section 3.

75. An "information handling provision" is defined in section 3 to mean "a provision of an Act that permits handling of personal information – (a) as authorised or required by law or by or under an Act; or in circumstances or for purposes required by law or by or under an Act". Where an approved IUA provides for the handling of personal information for the purposes of an information handling provision, the handling of that information in accordance with the arrangement is taken to be permitted for the purposes of that provision (section 51(2)). In this way, an IUA approved under the PDPA can override the limitations imposed on information sharing by information handling provisions in other Acts.

76. Pursuant to section 45(2), an IUA must:

76.1 specify the parties to the arrangements;

76.2 specify the personal information or type of personal information to be handled under the arrangement;

76.3 describe how the arrangement would facilitate one or more public purposes;

76.4 if the arrangement modifies or permits noncompliance with an IPP or approved code of practice, identify the relevant or code and state how it would be modified or not complied with;

76.5 identify and describe the effect of any relevant information handling provision;

76.6 for every party to the arrangement:

(a) describe the personal information or type of personal information that the party could disclose or transfer to other parties to the arrangement; and

(b) state the manner in which a party could use personal information, including whether a party could disclose that information to another person or body and in what circumstances;

76.7 for every organisation that is a party to the arrangement:

(a) state adverse actions (defined in s 43 to mean any action that may adversely affect the rights, benefits, privileges, obligations or interests or a specific individual) that an organisation could reasonably be expected to take as a result of handling personal information under the arrangement; and

(b) specify the procedure that an organisation must follow before taking adverse action as a result of handling of personal information under the arrangement.

77. An IUA can have one party or a number of parties, including private sector bodies, where a public sector organisation is the designated lead party. They are suitable for arrangements involving multiple parties and/or complex arrangements.

78. A lead party must apply for approval of an IUA by submitting it to the Commissioner. Approval of a proposed IUA is a two-step process:

78.1 first, the Commissioner must give consideration to the public interest in the proposal and prepare a report for the relevant Minister or Ministers and, where appropriate, certify that the proposal meets the public interest tests set out in section 49 of the PDPA; and

78.2 second, the relevant Minister or Ministers may, after receiving the Commissioner's report, approve an IUA if the Commissioner has issued a certificate in relation to it (section 50).

79. To date, my Office has not received any application for approval of an IUA. I have recently been contacted by the Department of Health and Human Services (**DHHS**) in relation to a proposed IUA for a family violence Risk Assessment and Management Panels (**RAMPs**) program that is being developed by the DHHS. I understand that the DHHS is in the process of preparing a Privacy Impact Assessment (which I will explain below) and the proposed IUA in relation to the RAMPs program and I expect to receive an application for approval of the proposed IUA from the DHHS, as the lead party for all of the organisations who will be involved in the RAMPs program, although no timeframe has been set.

80. I would like to respond to the evidence given to the Royal Commission by Professor Cathy Humphreys during the public hearing on 23 July 2015 in this regard. Professor Humphreys' suggestion that my involvement has somehow stopped the sharing of information in the two RAMPs pilot sites or stopped the further development of the RAMPs is incorrect. Prior to the recent contact from the DHHS, I have not had any involvement in the RAMPs pilots or the Statewide development of the RAMPs program and have not taken any action to inhibit information sharing within those programs. Consistent with my statutory functions as the Commissioner, with the objective of the PDPA to balance the public interest in the free flow of information with the public interest of protecting the privacy of individuals' personal information and with the views I have stated above of the equal importance of the confidentiality, integrity and *availability* of information in the data security context and in the family violence context specifically, I look forward to working constructively with the DHHS in relation to the application and approval of the proposed IUA relating to the RAMPs program.

Certification

81. Unlike the previous two mechanisms, certification does not permit or allow a departure from the IPPs or a code of practice. Rather, the certification mechanism is intended to address the situations frequently seen where appropriate information sharing may be hindered because organisations are uncertain about the interpretation of information sharing provisions in their legislation, or if there is disagreement between relevant organisations as to the correct interpretation of or interaction between provisions.

82. The certification mechanism provides that the Commissioner may certify that a specified act or practice of an organisation is consistent with an IPP, an approved code of practice or an information handling provision. If an organisation acts or engages in a practice in good faith in reliance on this certification, it will not contravene the relevant IPP, approved code of practice or information handling provision.

83. The Commissioner's decision to issue a certificate can be subject to review in the Victorian Civil and Administrative Tribunal upon the application of a person whose interests are affected.

84. To date, my Office has not received any application for certification under the PDPA.

OTHER LEGISLATIVE MODELS USED TO SUPPORT INFORMATION SHARING

85. My submission to the Royal Commission (Attachment DW-1, above) refers to several models that have been used to support information sharing. In this section of my statement, I provide some further detail about each of these models.

Human Services (Complex Needs) Act 2009 (Vic)

86. The purpose of the *Victorian Human Services (Complex Needs) Act 2009* is to facilitate the delivery of welfare services, health services, mental health services, disability services, drug and alcohol treatment services and housing and support services to certain persons with multiple and complex needs by providing for the assessment of such persons and the development and implementation of appropriate care plans.

87. This Act makes provision for the relevant Secretary to seek to obtain both personal information and health information about the person in question for the purposes of developing a care plan for that person, and specifies persons and entities authorised to disclose that personal or health information (section 14).

CARAM-DFV Framework (New South Wales)

88. On 30 June 2010, New South Wales adopted the 'CARAM-DFV Framework', which was effective for 12 months. The framework is described in the publication 'Cross Agency Risk Assessment and Management - Domestic and Family Violence Framework'. A Directive issued by the state's Information and Privacy Commission allowed public sector agencies and non-government organisations (NGOs)

operating within the CARAM-DFV Framework to assess victims of domestic and family violence as to the extent to which those victims were at risk of experiencing future violence.

89. This assessment was facilitated by the modification of the relevant Information protection Principles as specified in the Directive. In particular, paragraphs 6.29-6.31 exempted participating agencies from compliance with the restrictions on the disclosure of personal information about a third person in section 18 of the *Privacy and Personal Information Protection Act 1998* (NSW) for any of the following purposes (paragraph 6.29):

89.1 to undertake initial risk assessment, refer a victim for specialist risk assessment or undertake specialist risk assessment;

89.2 the provision of assistance and support services to the victim;

89.3 reporting any incident of domestic violence, that involves a serious threat of harm or physical injury which is likely to cause a reasonable victim to fear for her or his safety, to the NSW Police Force;

89.4 the evaluation of the trial of the CARAM-DFV Framework; or

89.5 any other purpose directly or indirectly related to the CARAM-DFV Framework.

90. Under the CARAM-DFV Framework, a participating agency could have disclosed personal information about a victim to the NSW Police Force if the agency believed on reasonable grounds that the disclosure was necessary to prevent or lessen a serious, but not necessarily imminent, threat to life, health or safety of the victim concerned or another person (paragraph 6.30).

91. The agencies participating in the CARAM-DFV Framework were the:

91.1 Departments of Health, Human Services, and Justice and Attorney-General;

91.2 New South Wales Police Force, established under the *Police Act 1990*;

91.3 Greater Southern Area Health Service; and

91.4 South Eastern Sydney and Illawarra Area Health Service.

92. I note that the above Direction stated that a related Direction had also been made under section 62 of the *Health Records and Information Privacy Act 2002* (NSW). The CARAM-DFV Framework expired in 2011, but was renewed in 2014 and expired on 30 June 2015. A copy of the Direction relating to the CARAM-DFV Framework published by the New South Wales Information and Privacy Commissioner is provided at **Attachment DW-11**.

Domestic Violence Disclosure Scheme (Clare's Law) (United Kingdom)

93. In the United Kingdom, following the 2009 murder of Clare Wood by her ex-partner, a new scheme was established to facilitate access to information where individuals are concerned that an individual may pose a risk to others in the context of domestic violence.

94. No new legislation has been introduced or police powers granted to enable this disclosure by police. The scheme works through the introduction of two types of processes:

94.1 the Right to Ask: this enables potential and actual victims, third parties such as parents, neighbours and friends, and agencies to make requests to police for information about individuals under the scheme; and

94.2 the Right to Know: this enables police to make a proactive decision to disclose details to potential victims when they receive information to suggest a person could be at risk.

95. My Office has prepared a Briefing note in relation to Clare's Law. A copy of this briefing note, *UK Domestic Violence Disclosure Scheme - Clare's Law* is provided at **Attachment DW-12**.

Approach taken in British Columbia

Legislative Framework

96. In 2011, British Columbia, Canada amended its *Freedom of Information and Protection of Privacy Act* (**FOIPPA**) to give public bodies clear ability to authorise the collection, use and disclosure of personal information for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur.

97. Despite arguments that existing provisions in FOIPPA, similar to those in the Victoria PDPA, would have enabled the sharing in most cases, it was believed that it was generally a misinterpretation or lack of understanding of the FOIPPA that prevented sharing. It was argued that it was necessary to change the Act to achieve a better awareness and to help workers be better informed in order to have the awareness necessary to proceed under the current Act to share the information that is necessary.

98. Prior to 2011, the collection and disclosure provisions in the FOIPPA were similar to IPP 1 and 2 in the PDPA. The revision to the FOIPPA in 2011 added a clear authority to collect, directly and indirectly, as well as disclose personal information to reduce the risk of family violence.

New Zealand

99. I have recently returned from New Zealand where I had discussions with a number of stakeholders in the family violence system. I am currently considering the implications of those discussions, including what aspects of that system would be of benefit in Victoria.

BARRIERS TO THE APPROPRIATE USE AND DISCLOSURE OF PERSONAL INFORMATION

100. I consider the key problems or inhibitors to the appropriate use and disclosure of personal information in Victoria to be:

100.1 a lack of agency or statutory legal authority to undertake functions involving the collection, use and disclosure of personal information;

100.2 statutory inhibitions or blockers on sharing personal information;

100.3 a poor understanding by agencies of how to work with privacy; and

100.4 cultural and ethical issues.

101. I will address each of these issues below as well as my recommendations as to how they could be overcome.

Lack of agency/statutory legal authority

102. As I have said above, the PDPA is default legislation: its information privacy provisions apply to the public sector except to the extent that they are inconsistent

with other legislation. The starting point for any public sector organisation is therefore to determine whether their enabling legislation permits the collection, use and disclosure of information. Some Government departments, such as the DHHS, administer several different enabling Acts. These departments and other public sector entities must have a thorough understanding of all relevant enabling legislation and the circumstances in which and extent to which the legislation permits the collection, use and disclosure of personal information. They can only share information that they have the legislative authority to share.

Statutory inhibitions/blockers

103. There may be specific legislative provisions, in a public sector organisation's enabling legislation or in other relevant Acts, which restrict the collection, use and disclosure of information. Examples include the types of confidentiality and secrecy provisions I have referred to above.

Poor understanding of how to work with privacy

104. It is only after consideration of these threshold issues that the privacy obligations in the PDPA and the *Health Records Act* come into play. In my experience, the difficulties experienced within some public sector organisations at different times in applying the privacy legislation derives in part from a poor understanding of how to work *with* privacy. Some of the reasons for this are:

104.1 failures to translate legal framework into the operating environment;

104.2 a lack of education and training; and

104.3 the structures of government encourage the segregation of functions and responsibilities.

105. In my role as the Commissioner, I have adopted an overarching approach to privacy, known as Privacy by Design, as a core policy to underpin information privacy management in the Victorian public sector and developed a number of tools to assist organisations and individuals within organisations to understand their privacy obligations and to facilitate the appropriate and timely disclosure of personal information.

Privacy by Design

106. Privacy by Design (**PbD**) is a methodology that aims to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information. It involves a level of intentionality regarding privacy management that marks a genuine departure from more common, well meaning but ad hoc approaches to privacy. PbD aims to shift the approach to privacy within the public sector from one of compliance, in which privacy is viewed as a compliance burden, to an approach which treats privacy as a "design feature" of public sector processes and activities by focusing on the design and operation of information systems throughout their life cycle.

107. I have developed a Background paper ("Privacy by Design: Effective Privacy Management in the Victorian public sector" (**Attachment DW-13**) (the **PbD Background Paper**) and a fact sheet ("Privacy by Design: The importance of a lifecycle approach involving people and programs" (**Attachment DW-14**)) relating to the PbD.

Privacy Impact Assessments

108. PbD involves the use of innovative approaches to privacy that are anchored in genuine respect for individuals' personal information. One of the most useful tools that can be used to implement PbD is a Privacy Impact Assessment (**PIA**). PIAs are explained at page 7 of the PbD Background Paper. In summary, a PIA is a point-in-time process that is designed to assist public sector organisations to identify and mitigate privacy risks and to identify and evaluate privacy solutions.

109. I have developed a Privacy Impact Assessment Template (**Attachment DW-15**) (**PIA Template**) to assist public sector organisations in conducting a PIA. I will provide further explanation of this process below in the section of my statement relating to the process that I recommend should be followed to address and overcome the barriers to information sharing in the family violence context.

110. PIAs should be used throughout the development and implementation of any project involving the collection and handling of personal information. Although conducting a PIA is not a mandatory legal requirement, it is my practice, as I state in the PbD Background Paper (at page 7), to require a PIA to be undertaken when public sector organisations seek to obtain a PID, an IUA or certification under the PDPA.

Checklist for Sharing Personal Information

111. I have also developed a Checklist for Sharing Personal Information (**Attachment DW-16**) which is designed to assist organisations to ask the right questions when considering both systematic and ad hoc requests for information sharing. The Checklist recommends that a PIA should always be undertaken to assess legislative authority to share and identify and mitigate privacy risks prior to sharing any personal information and that decisions to share information should be documented accordingly.

Guidelines to the IPPs

112. Further, as I have mentioned above, Guidelines to the Information Privacy Principles have been developed by the former Office of the Victorian Privacy Commissioner. These are attached to my statement at Attachment DW-8, above.

Cultural and ethical issues

113. Removing perceived legislative barriers does not ensure that information sharing will take place. In short, my experience is that there are many reasons why individuals refrain from sharing information. These include:

113.1 a general reluctance to share information;

113.2 an overly legalistic approach to information sharing;

113.3 professional or ethical obligations of confidentiality; and

113.4 concerns about sharing information in breach of their legislative obligations.

114. A culture of information sharing requires a willingness by public sector organisations to engage for a common purpose. I discuss my views about how to bring about cultural change in the following section of my statement.

RECOMMENDATIONS AS TO THE PROCESS FOR OVERCOMING BARRIERS TO INFORMATION SHARING IN THE FAMILY VIOLENCE CONTEXT

115. In this section of my statement, I make a number of recommendations as to the process that should be followed in order to overcome the barriers I have identified to information sharing in the family violence context.

Privacy Impact Assessment

116. The first step is for all of the public sector organisations involved in the provision of services in the family violence context, or a lead party representing all of the interested parties, to conduct a joint, comprehensive PIA addressing all information sharing issues in this context.

117. The PIA Template that I have developed (Attachment DW-15, above) will facilitate this process. The PIA Template requires the parties involved to identify the following matters in relation to the programs that are the subject of the PIA:

117.1 the parties involved, the roles that they perform as part of the program and the legal authority that each of them has to perform their role (Part 1.1);

117.2 the scope of the PIA (ie, the program or part of the program to which the PIA relates) and any related PIA (Part 1.2);

117.3 the information that is collected, used and disclosed, including any sensitive information (relevantly, in the context of family violence, this would include an individual's criminal record) and unique identifiers (such as a driver's licence) and whether any health information will be collected, used or disclosed (Part 1.3);

117.4 the information flows, which should set out (either in narrative form or in the form of a diagram) in as much detail as possible each element of personal information identified in Part 1 and how each element will be collected, used and disclosed, and by whom and to whom (Part 2.1);

117.5 how the IPPs apply to the information flows involved and the identification of any risks of noncompliance (Part 2.2);

117.6 the strategies and tools that will be implemented to mitigate each of the privacy risks identified (Part 3); and

117.7 a summary of the most significant findings and critical recommendations (Part 4).

118. The PIA that is being prepared by the DHHS in relation to the RAMPs program will provide a precedent for this process, but it is important to emphasise that the RAMPs program is only one of many multidisciplinary initiatives in the family violence context and, so far as I understand it, relates only to individuals at the

highest risk of serious injury or death. If the information flow within the RAMPs programs is limited to those circumstances and only to those parties in a position to lessen or prevent that risk, disclosure of personal information within the RAMPs would in my view be authorised by IPP 2.1(d)(i). However, the family violence context is much broader than this and the nature and degree of the risk to which victims are exposed is extremely varied and changeable.

119. This is an inevitably large and complex task. However, in my view, it is neither feasible nor desirable to conduct a separate PIA and apply for a separate IUA in relation to the many different programs designed to assess and manage risk across the broad spectrum of family violence cases. To the extent that it is possible to do so, there should be a single, comprehensive PIA conducted across the whole of the family violence system. That process would provide the parties involved with an informed knowledge base on which to identify an appropriate overarching solution to promote information sharing within the family violence context as a whole.

Potential features of an overarching family violence information sharing regime

120. While it is premature to make any definitive recommendations about what that overarching solution would look like, in my view the following considerations should be taken into account.

Modification of IPP 2.1(d)(i)

121. First, as I have noted above, IPP 2.1(d)(i) authorises the disclosure of personal information where an organisation reasonably believes that use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare. Risk is an inherently dynamic concept. It need not be "imminent" to constitute a serious and real threat to an individual's life or safety. In my view, a much greater degree of information sharing within the family violence context, and elsewhere, could be achieved by removing the requirement in IPP 2.1(d)(i) that the threat to an individual's life, health, safety or welfare be "imminent". This would be consistent with IPP 2.1(d)(ii), which authorises the disclosure of personal information where an organisation reasonably believes that use or disclosure is necessary to lessen or prevent a serious threat to public health, public safety or public welfare. There is no requirement of imminence.

Code of practice

122. Second, while IUAs provide a very useful mechanism for particular programs, they may not be appropriate for an overarching solution involving all public and non-public sector participants throughout the whole of the family violence system. Experience in New Zealand, from where the concept of IUAs in the PDPA is derived, suggests that where too many parties are involved, IUAs can become unwieldy. An alternative solution may be a sector-wide code of practice. Codes of practice may be made under Part 3 Division 3 of the PDPA by the Governor in Council, on the recommendation of the Minister acting on advice received from the Commissioner. Where an approved code of practice is in place, an organisation may discharge its duty to comply with an IPP by complying with the code (section 21(1)). No codes of practice have yet been approved under the PDPA or the predecessor legislation, the *Information Privacy Act*. In my view, that may be because a code of practice can not reduce the minimum protections prescribed by the IPPs (section 21(2)(a)).

123. Were the PDPA to be amended to permit codes of practice to depart from some or all of the minimum protections prescribed by the IPPs and any information handling provision, they could provide some flexibility for information sharing arrangements without the need for participants to be parties to an IUA.

124. A code of practice would also enable the IPPs, which are necessarily stated at a level of generality that is capable of application to the collection and handling of personal information in all contexts, to be contextualised to the family violence system and thereby provide more practical and workable information sharing practices between parties.

Application to health information

125. Third, the information privacy landscape could be simplified by ensuring that both personal and health information were covered in one piece of legislation. The main structural flaw in Victoria's information privacy approach is that personal information and health information are dealt with separately.

Need for detailed prescription

126. Fourth, I would be concerned about any broadly-framed legislative exemption for information sharing for the purposes of identifying and responding to the risk of family violence. In my view, any overarching arrangement – whether it be legislative amendment, a code of practice or an IUA – must contain sufficiently

detailed prescription about a range of matters relevant to information sharing, such as what information may be disclosed, to whom, in what circumstances, how it may be disclosed and the purposes for which recipients of information disclosed can subsequently use that information.

126.1 For example, if there are a number of service providers around a table as part of any multidisciplinary case management or referral program, not all of those service providers may have the requisite interest in information regarding some cases to justify its disclosure to them. For example, a Child Protection worker would not need to receive personal information about a family violence case in which there are no children involved.

126.2 As another example, a service provider may have information that suggests that an offender has been involved in criminal activity that, while it may be relevant to the assessment and management of the risk to a potential victim of family violence, is nevertheless not family violence-related offending. If such information were disclosed to Victoria Police, could the police use it to prosecute the offender?

127. Detailed provision would also ensure that the flow of information pursuant to such an overarching arrangement is transparent and capable of measurement through periodic reporting and auditing. This would promote compliance and enable an informed assessment of whether the arrangement continues to strike an appropriate balance between the public interest in maintaining the privacy of individuals' personal information and the public interest in the free flow of information necessary to reduce the incidence of family violence.

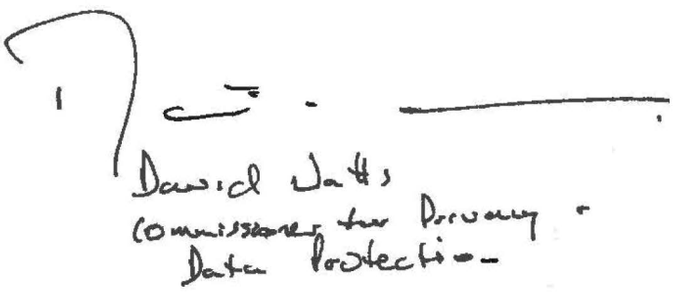
Cultural change

128. Finally, no overarching solution will be effective in promoting better information sharing in the family violence context in the absence of cultural change.

129. In my view, the starting point for achieving this change is for public sector organisations to engage with the Privacy by Design methodology that, as I have described above, enables public sector policy-makers and those responsible for delivering services to the community to approach privacy as a design feature of their processes and day to day activities, rather than as a compliance burden to be endured.

130. Cultural change will also require real commitment on the part of those in leadership positions within public sector organisations to bring about the necessary change. Among other things, this must involve a significant level of training of personnel from the highest level within any organisation down to those responsible for making decisions on a day to day basis to share or withhold information. It must also involve a "no blame" culture within public sector organisations, under which disclosures made in good faith but in breach of relevant privacy obligations do not result in adverse consequences for the individual concerned (albeit that the organisation itself may be exposed to liability to a third party for the wrongful disclosure).

Signed by)
DAVID GEOFFREY WATTS)
at Melbourne)
this 11th day of August 2015)



Before me

[redacted]

[redacted]

An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)