IN THE MATTER OF THE ROYAL COMMISSION INTO FAMILY VIOLENCE

ATTACHMENT DW-1 TO STATEMENT OF DAVID WATTS

Date of document: 31 July 2015
Filed on behalf of: the Applicant
Prepared by:
Victorian Government Solicitor's Office
Level 33
80 Collins Street
Melbourne VIC 3000

[redacted]

This is the attachment marked '**DW-1**' produced and shown to **DAVID WATTS** at the time of signing his Statement on 31 July 2015.

Before me: .... [redacted] .

[redacted]

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

Commissioner
for Privacy and
Data Protection

Response to Royal Commission into Family Violence Issues Paper 31 March 2015

Introduction

Although the Issues Paper does not specifically raise information privacy barriers – perceived or real – as impeding measures to prevent and/or respond to family violence, these issues are encompassed by questions 9 and 10.

The need to identify, reduce and prevent family violence, and ensure the safety of individuals affected by family violence requires integration and coordination between various organisations. This will regularly involve the sharing of sensitive personal information. Having the ability to share *the right information with the right people at the right time for the right purpose* will significantly supports better outcomes by protecting those at risk.

Privacy is sometimes cited as a barrier to necessary and appropriate information sharing. While it is important for government to protect the privacy rights of individuals, Victoria's privacy laws do not prevent the sharing of personal information where there is a serious threat to the health or safety of an individual or the public.

Privacy laws in Victoria have the capacity, when implemented properly, to enable information sharing in both emergency and day-to-day operational programs for the prevention and response to family violence.

That said, much needs to be done to ensure that the information sharing needs of frontline service delivery workers are clarified and simplified. This needs to occur *before* an emergency arises through the operationalisation of information sharing procedures – through, for example, training and standard operating procedures. Service delivery workers should not have to be lawyers.

What is Privacy?

Providing a conclusive definition of privacy is difficult. One of the main reasons for this is that it is a term that takes it's meaning from the context in which it is used.

The most general definition of privacy is freedom from interference or intrusion, or simply put, the right to be left alone. Privacy relates to principles of human dignity and integrity, human uniqueness, independence and the importance of solitude. Privacy is recognised as a human right in international instruments including the United Nations Declaration of Human Rights and the International Covenant on Civil and Political Rights. In Victoria, those international obligations are embodied in the Charter of Human Rights and Responsibilities Act 2006.

There are three classes of privacy that are commonly recognised – privacy of the person, territorial privacy and information privacy. Privacy of the person (or bodily privacy) protects an individual's bodily integrity, in particular the right not to have one's body touched or interfered with. For example, body

scans at an airport or drug testing at a place of employment may be considered by some as an invasion of bodily privacy. Territorial privacy (or spatial privacy) is concerned with placing limitations on the ability of one to intrude into another individual's personal space or environment. Invasion into an individual's territorial privacy may come in the form of video surveillance or ID checks.

The third class of privacy, information privacy, is the right of individuals to determine for themselves when, how, and to what extent their personal information is shared with others. This right is predicated on the assumption that an individual's personal information is fundamentally their own, and it is for them to choose freely whether to communicate their personal details as they see fit. Information privacy is concerned with establishing rules that govern the collection and handling of personal information by organisations, including both the public and private sector.

While all three classes of privacy are relevant in the context of family violence, information privacy and its impact on information sharing is of the most relevance. The privacy provisions of Victoria's *Privacy and Data Protection Act 2014* (PDPA) are primarily designed to protect information privacy within the Victorian public sector and outsourced service providers.

What is Information Security?

Victoria's privacy laws have always required the public sector to handle personal information securely. [1] The PDPA however, now enables the Commissioner to develop, oversee and monitor compliance with protective data security standards that will apply beyond personal information to government information generally. Although the Victorian Protective Data Security Framework has not yet been issued, it is at an advanced stage of development. It is built around three core pillars:

- Confidentiality – this means that information is not disclosed other than to those who have the authority to receive it
- Integrity – this is designed to ensure the trustworthiness or accuracy of information
- Availability – this means that authorised parties are able to access information when they need it

This configuration of principles is designed to support appropriate information sharing: that the right information is available to the right people at the right time. Victoria's information security framework is thus designed to support appropriate information sharing.

Legislation for Information Sharing in Victoria

Information sharing that takes place in Victoria, including for the purposes of preventing and responding to family violence, is based on the Information Privacy Principles (IPPs) that are codified in the PDPA. These principles are consistent with similar national and international laws. The IPPs protect the privacy of individuals by placing restrictions on how a public sector organisation collects, uses, discloses or otherwise handles personal information.

[1] See IPP 4

Victorian public sector organisations can collect personal information that is necessary for their functions or activities, and to use and disclose personal information for the primary purpose of collection or a secondary related purpose. Information that is collected by a public sector agency in connection with responding to family violence or providing a support service can generally be shared for that, or a similar purpose. In emergency situations, where individual or public health and safety is threatened, the PDPA permits the disclosure of personal information outside of these limitations.[2] When it comes to law enforcement agencies, the authority to use and disclose personal information is significantly expanded.[3]

The IPPs are in place to ensure that all individuals, especially those in vulnerable positions, have their informational privacy rights protected. However, in circumstances where it is unclear whether the authority to share information exists, the PDPA now includes flexibility mechanisms that were unavailable in the earlier *Information Privacy Act 2000,* that permit departures from certain IPPs when it is in the public interest to do so. These include:

- Public Interest Determinations
- Temporary Public Interest Determinations
- Information Usage Arrangements (IUAs)
- Certification[4]

An example of the use of powers such as these is the New South Wales Privacy Commissioner's Direction relating to Cross Agency Risk Assessment and Management – Domestic and Family Violence Framework.[5]

That said, public sector organisations need to be cognisant of requirements in their own enabling legislation. The PDPA only speaks to what personal information can be collected and disclosed where other legislation is silent. Confidentiality and secrecy provisions in legislation can impede information sharing. In their 2009 report, *Secrecy Laws and Open Government in Australia*, the Australian Law Reform Commission recommended that, for effective information handling, agencies need to develop and implement policies to clarify and harmonise the application of relevant secrecy laws to their information holdings.

Information Sharing for Family Violence in Victoria

The right to privacy does not trump the right to personal safety. Victoria's privacy laws are written to reflect that. Tragedies should not occur as a result of a misunderstanding of privacy legislation.

There is no question that a decision to disclose personal information without consent, whether that of a victim or an offender, can be difficult. Determinations often need to be made on a case-by-case basis. That said, our experience is that many Victorian public sector organisations have failed to properly operationalise their privacy, or other information obligations, including record-keeping obligations. Sometimes, this is attributable to them taking an excessively legalistic and risk-averse approach to information obligations. High quality service responses to family violence issues need to be supported

[2] See IPP 2.1
[3] See PDPA s 15
[4] See generally Divisions 5, 6 and 7 of the PDPA
[5] See http://ipc.nsw.gov.au/direction-relating-caram-dfv-framework

by high quality information sharing process and procedure, training and support so that front line workers can make decisions confidently and consistently.

The Need for Change

While there are some jurisdictions that have specifically incorporated authorities in their privacy legislation to enable information sharing for domestic and family violence (eg British Columbia, Canada), or have created separate legislation for this purpose (eg New South Wales, Australia), the standard privacy principles, such as the IPPs in the PDPA, should provide the required framework for appropriate information sharing. That said, we are aware of several models that have been used to support information sharing, including Clare's Law in the UK[6] and the *Human Services (Special Needs) Act 2009* (VIC). Legislation should not stand in the way of necessary information sharing – in other words, life trumps privacy.

Removing perceived legislative barriers does not ensure that information sharing will take place. A culture of information sharing requires a willingness by public sector organisations to engage for a common purpose. Accountability and transparency built into governance structures, coupled with collaborative approaches will create an environment ripe for appropriate, protected and timely information sharing. Ensuring the goal of sharing the right information with the right people at the right time for the right purpose requires a commitment to proactively consider information privacy and security and build these in at the design phase of systems, programs and processes. With planning and innovative thinking it should be possible to maintain good privacy and security, while enabling effective, efficient information sharing.

The Office of the Commissioner for Privacy and Data Protection would like to assist in this important area. Privacy should not be seen as a barrier to information sharing, and we want to help build a practical solution that authorises appropriate information sharing that is clearly and widely understood in the Victorian public sector.

David Watts
Commissioner for Privacy and Data Protection
29 May 2015

[6] Clare's Law is a misnomer as it is a combination of administrative and policy arrangements.