

Parliament of Victoria

Road Safety Committee - Inquiry into Serious Injury

Briefing from the Office of the Victorian Privacy Commissioner

28 October 2013

1. Introduction

The Victorian Parliament's Road Safety Committee received a reference from the Legislative Assembly in November 2012 to inquire into the nature and extent of crash related serious injury in Victoria.

Terms of reference (b) requires the Committee to:

identify processes, including the exchange of data and information between agencies, that will facilitate accurate, consistent and timely reporting of road related serious injuries.

The Committee has received evidence from various witnesses regarding how privacy laws currently limit the exchange of information and data between agencies, and how it may potentially limit the capacity for agencies to share data in the future for linking purposes.

2. The Victorian Public Sector Privacy Landscape

2.1 Victoria's *Information Privacy Act 2000 (IPA)* is the default regime that governs the collection, use, disclosure and other handling of personal information in the Victorian public sector. The IPA applies except to the extent that it is inconsistent with other more specific legislation (s6 IPA).

2.2 The IPA covers one important dimension of privacy – information privacy. Other aspects of privacy such as surveillance are covered in other legislation. Some other dimensions of privacy are not regulated at all except to the extent that they fall within s 13 of the *Charter of Human Rights and Responsibilities*.

2.3 The IPA only applies to personal information.

Personal information means:

Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose **identity is apparent, or can reasonably be ascertained**, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* applies. (s3 IPA, my emphasis)

To determine if an individual's identity is apparent or can reasonably be ascertained requires analysis of the information in question, the context and the circumstances of the case.

An individual's identity is 'apparent' when one could look at the information collected and know or perceive plainly and clearly that it was information about the individual.¹ For example, a photograph of an individual would satisfy this requirement.

Whether identity can be reasonably ascertained 'from the information or opinion' is a more difficult concept. Debate has centred on whether extraneous material can be taken into account, i.e., whether the requirement means ascertained solely from the information without reference to anything else. VCAT has suggested that the concept of 'ascertained' permits the use of some extraneous material or information.

2.4 The IPA is a principles-based regulatory regime that governs the collection, use disclosure and handling of personal information through a set of ten privacy principles known as the *Information Privacy Principles* (IPPs). A copy of the IPPs is Attachment 1.

2.5 Privacy is not regarded as an absolute right. It represents an important public interest that needs to be balanced against other interests. This approach is supported in the IPA's objects clause, section 5, which states that one of the objects of the IPA is '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.' The IPPs support this approach by enabling appropriate sharing of personal information IPP 2.1. This issue is covered in greater detail in the paragraph 5.

2.6 The IPA does not apply to health information. The collection, use, disclosure and handling of health information in the Victorian public sector is covered by the Victorian *Health Records Act 2001* and the Commonwealth's *Privacy Act 1988*. Health information would include information about the injuries sustained by an individual in a collision.

2.7 Finally, the Commonwealth legislation, the *Privacy Act 1988*, applies to the Commonwealth public sector and to parts of the private sector on a national basis. The *Privacy Act 1988* has recently been extensively amended. The amended legislation is due to come into effect in 2014.

3. Privacy is only one component of Victoria's information law landscape

3.1 A variety of laws, apart from privacy law, affect the collection and handling of information in the Victorian public sector. These include secrecy provisions in statutes, confidentiality obligations and specific statutory provisions that mandate the collection, use and disclosure of information in particular circumstances. An example of this is the provisions in Chapter 3 of the *Children, Youth and Families Act 2005* that permit or require certain categories of information sharing to support the safety and wellbeing of children.

3.2 A variety of other obligations that are not based in statute or common law are also relevant. These often take the form of ethical standards or codes of conduct. For the purposes of this Inquiry, the National Statement on Ethical Conduct in Human Research of October 2007 is particularly important because failure to comply with it means that research proposals will not be funded.

¹ OVPC, Guidelines to the Information Privacy Principles, edn 3, November 2011, p11

4 Criticisms of privacy

4.1 Privacy is criticised on a number of grounds. These include that it inhibits the appropriate sharing of personal information; that it impedes more efficient service delivery and that it discourages technological innovation.

4.2 Sometimes these criticisms have substance but on most occasions they do not. In many cases public sector agencies lack the skills to work with privacy and other information laws to support their existing and planned business processes. For many major ICT projects, the project focus is overwhelmingly technical and, in combination with project governance flaws, regulatory requirements are not sufficiently thought-through at a planning stage. Sometimes agencies do not wish to share information and use privacy as the justifying reason.

5. Sharing personal information

5.1 The IPA supports the appropriate sharing of personal information in a number of ways.

5.2 In general terms, the purpose for which information is collected establishes the boundaries for the use and disclosure (sharing) of that information. The primary rule is that personal information can be used and disclosed if the use and disclosure is for the primary purpose of collection. Secondary purposes are also permitted if they are sufficiently related to the primary purpose of collection and the individual would reasonably expect use and disclosure for the secondary purpose (IPP2.1(a)).

5.3 IPP2.1 also permits the disclosure of personal information in a number of other circumstances. One of these is IPP 2.1(c) which permits disclosure for the purposes of research, or the compilation or analysis of statistics in the public interest other than for publication in a form that identifies any particular individual.

5.3 Law enforcement agencies, such as Victoria Police, are exempt, under s 13 of the IPA, from a number of privacy requirements including the need to comply with IPP 2.1, if there is a belief on reasonable grounds that non-compliance is necessary for the purposes of law enforcement functions. This means that Victoria Police has significant scope to disclose (share) personal information.

5.4 One of the practical impediments to better information sharing is that public sector organisations do not have a uniform risk approach to information sharing issues: there are variations in their approach to the interpretation and application of privacy law leading to variations in the risk appetite of public sector organisations. In addition, they are required to take account of any particular legislative provisions relating to the information they collect and handle as well as the scope of their legal authority to do so.

6. Data Linkage

6.1 The Population Health Research Network (PHRN) defines data linkage as:

a method of bringing together information about people, places and events in a way that protects individual privacy. Using specially developed technology PHRN nodes will be linking existing information from different health and health related data collections to provide data to approved researchers for a range of population-based studies.²

6.2 A general description of the processes involved in data linkage is Attachment 2.

6.3 Data linkage is predominantly used in the context of health research and is designed to bring together a range of disparate data sets to assist population health research.

6.4 From a privacy perspective, the most significant challenges relate to questions involving the legal authority of the entity that leads the linkage project and the extent to which personal or health information is collected or disclosed.

6.5 The issue of legal authority is fundamental. Under privacy law, personal information may not be collected unless the collection is 'necessary for one or more' of the collecting organisation's functions or activities (IPP 1.1). IPP 1.3 requires organisations that collect personal information to take reasonable steps to make individuals whose personal information is collected aware of certain matters. These are set out in IPP 1.3 (a) – (f). Where a variety of disparate data sets are collected by a researcher, the researcher's legal authority to do so must be sufficiently broad.

6.6 Data linkage projects also aim to ensure that information that is collected, used and disclosed does not constitute personal or health information and thus is not covered by privacy or health privacy legislation either in whole or part. Data linkage involves the use of a number of terms of art such as 'anonymised' data, 're-identifiable data,' 'de-identified data' and 'non-identifiable data.' This vocabulary has no direct counterpart in the *legal* language of privacy legislation. As noted in paragraph 2.3, the key issue is whether or not personal information is collected, used and disclosed. Typically this involves determining if an individual's personal or health information is apparent or can be reasonably ascertained.

David Watts
A/Privacy Commissioner

² See <http://www.phrn.org.au/about-us/what-is-data-linkage>